

# Exhibit A

1 Hart L. Robinovitch (AZ SBN 020910)  
2 **ZIMMERMAN REED LLP**  
3 14646 North Kierland Blvd., Suite 145  
4 Scottsdale, AZ 85254  
5 Telephone: (480) 348-6400  
6 Facsimile: (480) 348-6415  
7 Email: hart.robinovitch@zimmreed.com

8 *Attorneys for Plaintiffs and the Class*  
9 *(Additional Counsel listed below)*

10 **UNITED STATES DISTRICT COURT**  
11 **DISTRICT OF ARIZONA**

12 Chris Griffey, Bharath Maduranthgam  
13 Rayam, and Michael Domingo,  
14 individually and on behalf of all others  
15 similarly situated,

16 Plaintiffs,

17 -v-

18 Magellan Health, Inc., a Delaware  
19 corporation,

20 Defendant.

Case No. CV-19-01228-PHX-SMB

**CLASS ACTION COMPLAINT**

**DEMAND FOR JURY TRIAL**

21  
22  
23  
24  
25  
26  
27  
28

1 Plaintiffs CHRIS GRIFFEY, BHARATH MADURANTHGAM RAYAM  
2 (“Plaintiffs”), individually, and on behalf of all others similarly situated, bring this action  
3 against Defendant, MAGELLAN HEALTH, INC. (“Magellan Health” or “Defendant”)  
4 to obtain damages, restitution, and injunctive relief for the Class, as defined below, from  
5 Defendant. Plaintiffs make the following allegations upon information and belief, except  
6 as to their own actions, the investigation of their counsel, and the facts that are a matter  
7 of public record:

8 **I. PARTIES**

9 1. Plaintiff BHARATH MADURANTHGAM RAYAM is, and at all times  
10 mentioned herein was, an individual citizen of the state of Tennessee residing in the city  
11 of Nashville. RAYAM was employed by Magellan Health during the period March 16,  
12 2020 through May 8, 2020. Plaintiff Rayam received notice of the data breach, and a  
13 copy of the notice is attached hereto as Exhibit A.

14 2. Plaintiff CHRIS GRIFFEY is, and at all times mentioned herein was, an  
15 individual citizen of the state of Missouri residing in the city of Wildwood. GRIFFEY  
16 was employed by Magellan Health during the period December 12, 2011 through July  
17 6, 2016. Plaintiff Griffey received notice of the data breach, and a copy of the notice is  
18 attached hereto as Exhibit B.

19 3. Plaintiff MICHAEL DOMINGO is, and at all times mentioned herein was,  
20 an individual citizen of the state of Pennsylvania residing in the city of Jamison.  
21 DOMINGO was employed by Magellan Health during the period through August 2016  
22 through February 29, 2020. Plaintiff Domingo received notice of the data breach, and a  
23 copy of the notice is attached hereto as Exhibit C.

24 4. Defendant Magellan Health is a publicly traded Delaware corporation  
25 headquartered at 4801 E. Washington Street, Phoenix, Arizona 85034. It is a Fortune  
26 500 company broadly operating in the healthcare management business.

**II. JURISDICTION**

1  
2 5. This Court has jurisdiction over this action under the Class Action Fairness  
3 Act (“CAFA”), 28 U.S.C. § 1332(d). There are at least 100 members in the proposed  
4 class, the aggregated claims of the individual Class Members exceed the sum or value of  
5 \$5,000,000.00 exclusive of interest and costs, and members of the Proposed Class are  
6 citizens of states different from Defendant.

7 6. This Court has jurisdiction over Defendant, which operates and is  
8 headquartered in this District. The computer systems implicated in this Data Breach are  
9 likely based in this District. Through their business operations in this District, Magellan  
10 intentionally avails itself of the markets within this District to render the exercise of  
11 jurisdiction by this Court just and proper.

12 7. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a  
13 substantial part of the events and omissions giving rise to this action occurred in this  
14 District. Defendant is based in this District, maintains the personally identifiable  
15 information (“PII”) and protected health information (“PHI”) of Plaintiffs and Class  
16 members in this District, and has caused harm to Plaintiffs and Class Members through  
17 its actions in this District.

**III. NATURE OF THE ACTION**

18  
19 8. This class action arises out of the most recent targeted cyberattack and data  
20 breach (“Data Breach”) involving Magellan Health. As a result of the Data Breach, the  
21 PII and PHI of Plaintiffs and at least 163,654 Class members is in the hands of  
22 cyberthieves. Plaintiffs and Class Members suffered ascertainable losses in the form of  
23 out-of-pocket expenses and the value of their time reasonably incurred to remedy or  
24 mitigate the effects of the attack. In addition, Plaintiffs’ and Class members’ sensitive  
25 personal information—which was entrusted to Magellan Health, its officials and  
26 agents—was compromised and unlawfully accessed due to the Data Breach. Information  
27 compromised in the Data Breach included names, contact information, employee ID  
28 numbers, and W-2 or 1099 information, including Social Security numbers or taxpayer

1 identification numbers, treatment information, health insurance account information,  
2 member IDs, other health-related information, email addresses, phone numbers, physical  
3 addresses, and additional PII.

4 9. Plaintiffs bring this class action lawsuit on behalf of those similarly situated  
5 to address Defendant's inadequate safeguarding of Class Members' PII and PHI that it  
6 collected and maintained, and for failing to provide timely and adequate notice to  
7 Plaintiffs and other Class members that their information had been subject to the  
8 unauthorized access of an unknown third party and precisely what specific type of  
9 information was accessed.

10 10. Defendant maintained the PII and PHI in a reckless manner. In particular,  
11 the PII and PHI was maintained on Defendant Magellan Health's computer network in a  
12 condition vulnerable to cyberattacks. The mechanism of the cyberattack and potential  
13 for improper disclosure of Plaintiffs' and Class members' PII and PHI was a known risk  
14 to Defendant, as it was subject to another data breach a mere 11 months prior that  
15 involved another phishing attack, and thus Defendant was on notice that failing to take  
16 steps necessary to secure the PII and PHI from those risks left that property in a dangerous  
17 condition.

18 11. In addition, Magellan Health and its employees failed to properly monitor  
19 the computer network and systems that housed the PII and PHI. Had Magellan Health  
20 properly monitored its property, it would have discovered the intrusion sooner.

21 12. Plaintiffs' and Class members' identities are now at risk because of  
22 Defendant's negligent conduct since the PII and PHI that Defendant Magellan Health and  
23 its affiliates collected and maintained is now in the hands of data thieves.

24 13. Armed with the PII and PHI accessed in the Data Breach, data thieves can  
25 commit a variety of crimes including, e.g., opening new financial accounts in Class  
26 members' names, taking out loans in Class members' names, using Class members'  
27 names to obtain medical services, using Class members' health information to target  
28 other phishing and hacking intrusions based on their individual health needs, using Class

1 members' information to obtain government benefits, filing fraudulent tax returns using  
2 Class members' information, obtaining driver's licenses in Class members' names, but  
3 with another person's photograph, and giving false information to police during an arrest.

4 14. As a result of the Data Breach, Plaintiffs and Class members have been  
5 exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class  
6 members must now and in the future closely monitor their financial accounts to guard  
7 against identity theft.

8 15. Plaintiffs and Class members may also incur out of pocket costs for, e.g.,  
9 purchasing credit monitoring services, credit freezes, credit reports, or other protective  
10 measures to deter and detect identity theft.

11 16. By their Complaint, Plaintiffs seek to remedy these harms on behalf of  
12 themselves and all similarly situated individuals whose PII was accessed during the Data  
13 Breach.

14 17. Plaintiffs seek remedies including, but not limited to, compensatory  
15 damages, reimbursement of out-of-pocket costs, and injunctive relief including  
16 improvements to Defendant's data security systems, future annual audits, and adequate  
17 credit monitoring services funded by Defendant.

18 18. Accordingly, Plaintiffs bring this action against Defendant seeking redress  
19 for its unlawful conduct, and asserting claims for: (i) negligence; (ii) negligence *per se*;  
20 (iii) unjust enrichment; (iv) breach of implied contract, and; (v) violation of the Arizona  
21 Consumer Fraud Act.

#### 22 **IV. STATEMENT OF FACTS**

##### 23 **A. Defendant Magellan Health.**

24 19. Defendant Magellan Health is a for-profit managed health care company,  
25 focused on special populations, complete pharmacy benefits and other specialty areas of  
26 healthcare. It directly manages health benefits for its members' patients, including those  
27 of its affiliates/subsidiaries Magellan Complete Care of Florida, Magellan Rx Pharmacy  
28 of Maryland, and Magellan Complete Care of Virginia, LLC.

1           20. As part of its contractual relationship with the aforementioned  
2 affiliates/subsidiaries and several other providers, Defendant administers the health and  
3 pharmaceutical benefits offered by those affiliates/subsidiaries. Defendant Magellan  
4 Health received fees from these affiliates or the states in which they operate to administer  
5 those benefits and to provide services related to those benefits to Class members, which  
6 included storing the personal data of Class members on its computers and computer  
7 systems. The fees received by Defendant for these services are accrued and paid as a  
8 result of Class members' participation in and payment for these health and  
9 pharmaceutical plans.

10 **B. The Data Breach.**

11           21. A ransomware attack deploys a type of malicious software that blocks  
12 access to a computer system or data, usually by encrypting it, until the victim pays a fee  
13 to the attacker.<sup>1</sup>

14           22. In April 2020, Magellan Health was struck by a targeted cyberattack, by  
15 way of email phishing scheme expressly designed to gain access to private and personal  
16 data stored by Magellan Health.

17           23. The ransomware attack was detected by Magellan Health on April 11, 2020  
18 when files were encrypted on its systems. The investigation into the attack revealed the  
19 attacker had gained access to its systems following a response to a spear phishing email  
20 sent on April 6.

21           24. A Magellan Health employee inappropriately responded to the email  
22 phishing scheme, allowing unauthorized actors to gain access to the employees' email  
23 accounts.

24           25. The Data Breach was a direct result of Defendant's failure to implement  
25 adequate and reasonable cyber-security procedures and protocols necessary to protect PII  
26 and PHI, including the PII of its employees (including Plaintiffs) and the PII and PHI of  
27 participants in the health and pharmaceutical plans of the aforementioned

28 <sup>1</sup><https://www.proofpoint.com/us/threat-reference/ransomware>.

1 affiliates/subsidiaries.

2 26. On or about May 12, 2020, Magellan Health notified affected persons and  
3 various governmental agencies of the Data Breach. The Notice of Data Incident  
4 (“Notice”) stated in relevant part the following:

5 **Notice of Data Incident**

6 *What Happened*

7  
8 On April 11, 2020, Magellan Health discovered it was targeted by a  
9 ransomware attack. The unauthorized actor gained access to Magellan  
10 Health’s systems after sending a phishing email on April 6 that impersonated  
11 a Magellan Health client. Once the incident was discovered, Magellan Health  
12 immediately retained a leading cybersecurity forensics firm, mediation to  
13 help conduct a thorough investigation of the incident. The investigation  
14 revealed that prior to the launch of the ransomware, the unauthorized actor  
15 exfiltrated a subset of data from a single Magellan Health corporate server,  
16 which included some of your personal information. In limited instances, and  
17 only with respect to certain current employers, the unauthorized actor also  
18 used a piece of malware designed to steal login credentials and passwords.  
19 At this point, we are not aware of any fraud or misuse of your personal  
20 information as a result of this incident, but we are notifying you out of an  
21 abundance of caution.

22 *What Information Was Involved*

23 The exfiltrated records include personal information such as names, address,  
24 employee ID number, and W-2 OR 1099 details such as Social Security  
25 number of Taxpayer ID number and, in limited circumstances, may also  
26 include usernames and passwords

27 *What We Are Doing*

28 Magellan Health immediately reported the incident to , and is working  
closely with, the appropriate law enforcement authorities, including the FBI.  
Additionally, to help prevent a similar type of incident from occurring in the  
future , we implemented additional security protocols designed to protect out  
network, email environment, systems, and personal information.<sup>2</sup>

29 27. Upon information and belief, this notice was sent to 50410 persons, and

---

<sup>2</sup> <https://oag.ca.gov/system/files/Magellan%20-%20Sample%20Individual%20Notice.pdf>



1 was reported to the US Department of Health and Human Services on June 12, 2020.

2 28. On June 12, 2020, Defendant subsequently issued a second notice of data  
3 breach to the plan participants of Complete Care of Florida and Magellan Rx Pharmacy  
4 of Maryland, and reported the data breach for Magellan Health to HHS. This notice was  
5 sent to 76236 plan participants of Complete Care of Florida, and 33040 plan participants  
6 of Magellan Rx Pharmacy of Maryland.

7 29. This second notice of data breach states, in pertinent part:

8 *Notice of Security Incident*

9 Magellan Health, Inc. and its subsidiaries and affiliates (“Magellan”) recently discovered a ransomware attack. We are providing notice of this  
10 incident, along with background information of the incident and steps that  
11 those affected can take.

12 *What Happened*

13  
14 On April 11, 2020 we discovered that we were the target of a ransomware  
15 attack. Immediately after discovering the incident we retained a leading  
16 cybersecurity forensics firm, Mandiant, to help conduct a thorough  
17 investigation of the incident. The investigation revealed that the incident  
18 may have affected personal information.

19 **We have no evidence that any personal data has been misused.**

20 *What Information Was Involved*

21 The personal information included names and one or more of the following:  
22 treatment information, health insurance account information, member ID,  
23 other health-related information, email addresses, phone numbers, and  
24 physical addresses. In certain instances, Social Security numbers were also  
25 affected.

26 *What Are We Doing*

27 We immediately reported the incident to, and are working closely with, law  
28 enforcement including the FBI. To help prevent a similar incident from  
occurring in the future, we have implemented additional security protocols  
designed to protect our network, email environment, systems, and personal  
information.

1 A copy of this second notice is posted on Defendant's website.<sup>3</sup>

2 30. While clearly related to the same ransomware attack and Data Breach as  
3 the May 15, 2020 Notice, the June 12, 2020 notice varies markedly from the May notice,  
4 in that the June 12, 2020 notice provides far less information about the specific facts of  
5 the cyberattack, does not mention the exfiltration of data that the May notice admits, and  
6 does not offer any credit monitoring option to the persons to whom the notice was sent.

7 31. On June 15, 2020, Defendant issued a notice identical in form to the June  
8 12, 2020 notice to persons affected by this Data Breach who were plan participants of  
9 Defendant's affiliate/subsidiary Magellan Complete Care of Virginia, LLC, and reported  
10 the data breach for that affiliate to HHS on that same date.

11 32. This is the second cyberattack in less than a year that Defendant Magellan  
12 allowed to happen through inadequate email handling procedures and other data security  
13 deficiencies. On May 28, 2019, an unauthorized third party gained access to a Magellan  
14 employee email account through a commonplace phishing attack that resulted in the  
15 exposure of sensitive patient PHI and PII. Magellan gave notice of this prior data breach  
16 on or about November 8, 2019. Magellan is already the subject of another lawsuit  
17 pending in the United States District Court for the District of Arizona, Phoenix Division,  
18 styled Deering v. Magellan Health, Inc. et al., Case 2:20-cv-00747-SPL (4/17/2020),  
19 arising out of that prior data breach.<sup>4</sup>

20 **C. Magellan Health's Employment Data Protection Standards**

21 33. Magellan Health has established a Privacy Policy wherein it details the PII  
22 it collects from employees and its standards to maintain the security and integrity of such  
23  
24  
25

26 <sup>3</sup> <https://www.magellanhealth.com/news/security-incident/>

27 <sup>4</sup> This action and the prior lawsuit are not related, as they arise from two separate  
28 incidents.

1 data.<sup>5</sup>

2 34. The aim of the Privacy Policy is to provide adequate and consistent  
3 safeguards for the handling of employment data by Magellan Health.

4 **D. Magellan Health’s Patient Privacy Policies.**

5 35. As a healthcare service provider, Defendant Magellan Health is bound by  
6 the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), which  
7 requires subject providers to comply with a series of administrative, physical security,  
8 and technical security requirements in order to protect patient information. Among other  
9 things, it mandates that medical providers develop, publish, and adhere to a privacy  
10 policy.

11 36. Defendant recognizes its obligations under HIPAA along with the  
12 commensurate obligation to safeguard and protect patient PHI and PII:

13 HIPAA outlines strict guidelines to ensure the privacy and confidentiality of  
14 your Personal Health Information (PHI) such as your name or medical  
15 information. These guidelines require that your PHI be used for purposes of  
16 treatment, payment and health plan operations, and not for purposes  
unrelated to health care.<sup>6</sup>

17 37. Defendant assures consumers that “[y]our personal privacy is important to  
18 us.”<sup>7</sup> Magellan Health’s Privacy Policy further states: “Magellan uses physical, technical,  
19 and administrative safeguards to protect any personally identifiable data stored on its  
20  
21

22  
23 <sup>5</sup> <https://www.magellanhealth.com/privacy-policy/#:~:text=Magellan Health%20uses%20physical%2C%20technical%2C%20and,for%20providing%20service%20to%20you>. (last visited June 25, 2020).

24 <sup>6</sup> <https://www.magellancompletecareoffl.com/utility/privacy-policy/> (last visited  
25 6/28/2020)

26 <sup>7</sup> [https://www.magellanhealth.com/privacy-  
27 policy/#:~:text=Magellan%20uses%20physical%2C%20technical%2C%20and,for%20providing%20service%20to%20you](https://www.magellanhealth.com/privacy-policy/#:~:text=Magellan%20uses%20physical%2C%20technical%2C%20and,for%20providing%20service%20to%20you) (last visited 6/28/2020)  
28

1 computers. Only authorized employees and third parties have access to the information  
2 you provide to Magellan for providing service to you.”<sup>8</sup>

3 **E. Prevalence of Cyber Attacks and Susceptibility of the Data Storage Industry.**

4 38. Data breaches have become widespread. In 2016, the number of U.S. data  
5 breaches surpassed 1,000, a record high and a forty percent increase in the number of  
6 data breaches from the previous year. In 2017, a new record high of 1,579 breaches were  
7 reported, representing a 44.7 percent increase over 2016. In 2018, there was an extreme  
8 jump of 126 percent in the number of consumer records exposed from data breaches. In  
9 2019, there was a 17 percent increase in the number of breaches (1,473) over 2018, with  
10 164,683,455 sensitive records exposed.<sup>9</sup>

11 39. What’s more, companies in the business of storing and maintaining PII,  
12 such as Magellan Health are among the most targeted—and therefore at risk—for  
13 cyber-attacks.<sup>10</sup>

14 **F. Prevalence of Cyber Attacks and Susceptibility of the Healthcare Industry.**

15 40. The healthcare industry is even more at known risk of cyber-attack. The  
16 number of data breaches in the healthcare sector skyrocketed in 2019, with 525 reported  
17 breaches exposing nearly 40 million sensitive records (39,378,157), compared to only  
18 369 breaches that exposed just over 10 million sensitive records (10,632,600) in 2018.<sup>11</sup>

19 41. Phishing cyberattacks against healthcare organizations are targeted.  
20 According to the 2019 Health Information Management Systems Society, Inc.  
21 (“HIMMS”) Cybersecurity Survey, “[a] pattern of cybersecurity threats and experiences

---

22 <sup>8</sup> *Id.*

23 <sup>9</sup> <https://www.idtheftcenter.org/identity-theft-resource-centers-annual-end-of-year-data-breach-report-reveals-17-percent-increase-in-breaches-over-2018/>

25 <sup>10</sup> <https://www.cshub.com/attacks/articles/top-8-industries-reporting-data-breaches-in-the-first-half-of-2019>

27 <sup>11</sup> [https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020\\_ITRC\\_2019-End-of-Year-Data-Breach-Report\\_FINAL\\_Highres-Appendix.pdf](https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf)

1 is discernable across US healthcare organizations. Significant security incidents are a  
2 near-universal experience in US healthcare organizations with many of the incidents  
3 initiated by bad actors, leveraging e-mail as a means to compromise the integrity of their  
4 targets.”<sup>12</sup> “Hospitals have emerged as a primary target because they sit on a gold mine  
5 of sensitive personally identifiable information for thousands of patients at any given  
6 time. From Social Security and insurance policies to next of kin and credit cards, no other  
7 organization, including credit bureaus, have so much monetizable information stored in  
8 their data centers.”<sup>13</sup>

9 42. The exposure of highly personal and highly confidential healthcare  
10 related data is of great consequence to patients. As the ID Theft Center notes:

11 Medical identity theft is costly to consumers. Unlike credit-card fraud,  
12 victims of medical identity theft can suffer significant financial  
13 consequences. Sixty-five percent of medical identity theft victims had to pay  
14 an average of \$13,500 to resolve the crime. In some cases, they paid the  
15 health care provider, repaid the insurer for services obtained by the thief, or  
16 they engaged an identity-service provider or legal counsel to help resolve the  
17 incident and prevent fraud.

18 Those who have resolved the crime spent, on average, more than 200 hours  
19 on such activities as working with their insurer or health-care provider.

20 Medical identity theft can have a negative impact on reputation. Forty-five  
21 percent of respondents said medical identity theft affected their reputation  
22 mainly because of embarrassment due to disclosure of sensitive personal  
23 health conditions; 19 percent of respondents believed the theft caused them  
24 to miss out on career opportunities. Three percent said it resulted in the loss  
25 employment.<sup>14</sup>

---

25 <sup>12</sup> <https://www.himss.org/himss-cybersecurity-survey> (last accessed June 20, 2020)

26 <sup>13</sup> <https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks> (last accessed June 20, 2020)

27 <sup>14</sup> <https://www.idtheftcenter.org/medical-id-theft-costs-victims-big-money/#:~:text=Medical%20identity%20theft%20is%20costly,%2413%2C500%20to%20resolve%20the%20crime.> (last accessed June 20, 2020)

1 **G. Defendant Acquires, Collects, and Stores Plaintiffs’ and Class Members’ PII**  
2 **and PHI.**

3 43. As its Privacy Policy makes clear, Magellan Health acquires, collects, and  
4 stores a massive amount of personally identifiable information (“PII”) on its employees,  
5 former employees and beneficiaries.

6 44. As a condition of employment, or as a condition of receiving certain  
7 benefits, Magellan Health requires that its employees and their beneficiaries entrust it  
8 with highly sensitive personal information.

9 45. Defendant also required and Class Members to submit non-public personal  
10 information, PII, and PHI in order to obtain medical and pharmacy services from its  
11 affiliates, and also creates PHI (e.g. treatment records) in the course of providing medical  
12 and pharmacy services.

13 46. By obtaining, collecting, creating, and using, Plaintiffs’ and Class  
14 Members’ PII and PHI, Defendant assumed legal and equitable duties and knew or should  
15 have known that it was responsible for protecting Plaintiffs’ and Class Members’ PII and  
16 PHI from disclosure.

17 47. Plaintiffs and the Class Members have taken reasonable steps to maintain  
18 the confidentiality of their PII and PHI.

19 48. Plaintiffs and the Class Members relied on Defendant to keep their PII and  
20 PHI confidential and securely maintained, to use this information for business purposes  
21 only, and to make only authorized disclosures of this information.

22 **H. The Value of Personally Identifiable Information and the Effects of**  
23 **Unauthorized Disclosure**

24 49. Defendant Magellan Health was well-aware that the PII and PHI it  
25 collected is highly sensitive, and of significant value to those who would use it for  
26 wrongful purposes.

27 50. Personally identifiable information is a valuable commodity to identity  
28 thieves. As the FTC recognizes, with PII identity thieves can commit an array of

1 crimes including identify theft, medical and financial fraud.<sup>15</sup> Indeed, a robust “cyber  
2 black market” exists in which criminals openly post stolen PII on multiple underground  
3 Internet websites.

4 51. The ramifications of Defendant’s failure to keep Plaintiffs’ and Class  
5 Members’ PII secure are long lasting and severe. Once PII is stolen, fraudulent use of  
6 that information and damage to victims may continue for years.

7 52. At all relevant times, Defendant knew, or reasonably should have known,  
8 of the importance of safeguarding PII and of the foreseeable consequences if its data  
9 security systems were breached, including, the significant costs that would be imposed  
10 on employees and their beneficiaries as a result of a breach.

11 53. Defendant breached its obligations to Plaintiffs and Class Members and/or  
12 was otherwise negligent and reckless because it failed to properly maintain and safeguard  
13 the computer systems and data that held the stolen PII. Defendant’s unlawful conduct  
14 includes, but is not limited to, the following acts and/or omissions:

- 15 a. Failing to maintain an adequate data security system to reduce the risk of  
16 data breaches and cyber-attacks;
- 17 b. Failing to adequately protect consumers’ PII and PHI;
- 18 c. Failure to periodically ensure that their email system had plans in place to  
19 maintain reasonable data security safeguards;
- 20 d. Allowing unauthorized access to Plaintiffs’ and Class Members’ PII and  
21 PHI;
- 22 e. Failing to properly monitor the data security systems for existing  
23 intrusions, and;
- 24 f. Failing to ensure that its agents and service providers with access to  
25 Plaintiffs’ and Class Members’ PII and PHI employed reasonable security  
26 procedures.

27  
28 <sup>15</sup> Federal Trade Commission, *Warning Signs of Identity Theft*,  
<https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft>

1           54. It was foreseeable that Defendant’s failure to use reasonable measures to  
2 protect Class Members’ PII and PHI would result in injury to Class Members. Further,  
3 the breach of security was reasonably foreseeable given the known high frequency of  
4 cyberattacks and data breaches in the data storage and healthcare industries.

5           55. It was therefore foreseeable that the failure to adequately safeguard Class  
6 Members’ Private Information would result in one or more types of injuries to Class  
7 Members.

8 **I. Defendant Failed to Comply with FTC Guidelines.**

9           56. The Federal Trade Commission (“FTC”) has promulgated numerous  
10 guides for businesses which highlight the importance of implementing reasonable data  
11 security practices. According to the FTC, the need for data security should be factored  
12 into all business decision-making.<sup>16</sup>

13           57. In 2016, the FTC updated its publication, *Protecting Personal Information:*  
14 *A Guide for Business*, which established cyber-security guidelines for businesses.<sup>17</sup> The  
15 guidelines note that businesses should protect the personal customer information that they  
16 keep; properly dispose of personal information that is no longer needed; encrypt  
17 information stored on computer networks; understand their network’s vulnerabilities; and  
18 implement policies to correct any security problems. The guidelines also recommend that  
19 businesses use an intrusion detection system to expose a breach as soon as it occurs;  
20 monitor all incoming traffic for activity indicating someone is attempting to hack the  
21 system; watch for large amounts of data being transmitted from the system; and have a  
22 response plan ready in the event of a breach.

23           58. The FTC further recommends that companies not maintain PII longer than  
24 is needed for authorization of a transaction; limit access to sensitive data; require complex  
25

---

26 <sup>16</sup> Federal Trade Commission, *Start With Security*, available at  
27 [https://www.ftc.gov/system/files/documents/plain-language/pdf0205-  
startwithsecurity.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf).

28 <sup>17</sup> [https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-  
information-guide-business](https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business)



1 passwords to be used on networks; use industry-tested methods for security; monitor for  
2 suspicious activity on the network; and verify that third-party service providers have  
3 implemented reasonable security measures.<sup>18</sup>

4 59. The FTC has brought enforcement actions against businesses for failing to  
5 adequately and reasonably protect customer data, treating the failure to employ  
6 reasonable and appropriate measures to protect against unauthorized access to  
7 confidential consumer data as an unfair act or practice prohibited by Section 5 of the  
8 Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these  
9 actions further clarify the measures businesses must take to meet their data security  
10 obligations.

11 60. Defendant failed to properly implement basic data security practices.  
12 Defendant’ failure to employ reasonable and appropriate measures to protect against  
13 unauthorized access to consumer PII and PHI constitutes an unfair act or practice  
14 prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

15 61. Defendant was at all times fully aware of its obligation to protect the PII of  
16 consumers. Defendant was also aware of the significant repercussions that would result  
17 from its failure to do so.

18 **J. Defendant Failed to Comply with Industry Standards.**

19 62. Companies in the business of storing and maintaining PII and PHI, such as  
20 Magellan Health, have been identified as being particularly vulnerable to cyber-attacks  
21 because of the value of the PII and PHI which they maintain. Cybersecurity firms have  
22 promulgated a series of best practices that a minimum should be implemented by sector  
23 participants including, but not limited to: installing appropriate malware detection  
24 software; monitoring and limiting the network ports; protecting web browsers and email  
25 management systems; setting up network systems such as firewalls, switches and routers;

26  
27 <sup>18</sup> Federal Trade Commission, *Start With Security*, available at  
28 <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>.

1 monitoring and protection of physical security systems; protection against any possible  
2 communication system; and training staff regarding critical points.<sup>19</sup>

3 63. The Data Breach appears to have been caused by “a standard credential  
4 phishing attack or due to credential reuse on another site.”<sup>20</sup>

5 64. Cybersecurity experts have explicitly noted that phishing attacks can be  
6 prevented with adequate staff security training.<sup>21</sup>

### 7 **K. Plaintiffs and Class Members Suffered Damages**

8 65. The ramifications of Defendant’s failure to keep employees’ PII and PHI  
9 secure are long lasting and severe. Once PII is stolen, fraudulent use of that information  
10 and damage to victims may continue for years. Consumer victims of data breaches are  
11 more likely to become victims of identity fraud.

12 66. The PII and PHI belonging to Plaintiffs and Class Members is private,  
13 sensitive in nature, and was left inadequately protected by Defendant who did not obtain  
14 Plaintiffs’ or Class Members’ consent to disclose such PII to any other person as required  
15 by applicable law and industry standards.

16 67. The Data Breach was a direct and proximate result of Defendant’s failure  
17 to: (a) properly safeguard and protect Plaintiffs’ and Class Members’ PII and PHI from  
18 unauthorized access, use, and disclosure, as required by various state and federal  
19 regulations, industry practices, and common law; (b) establish and implement appropriate  
20 administrative, technical, and physical safeguards to ensure the security and  
21 confidentiality of Plaintiffs’ and Class Members’ PII; and (c) protect against reasonably  
22 foreseeable threats to the security or integrity of such information.

23  
24  
25 <sup>19</sup> <https://insights.datamark.net/addressing-bpo-information-security/>

26 <sup>20</sup> [https://www.scmagazine.com/home/security-news/phishing/canon-breach-exposes-](https://www.scmagazine.com/home/security-news/phishing/canon-breach-exposes-personal-data-of-current-former-ge-employees-beneficiaries/)  
27 [personal-data-of-current-former-ge-employees-beneficiaries/](https://www.scmagazine.com/home/security-news/phishing/canon-breach-exposes-personal-data-of-current-former-ge-employees-beneficiaries/).

28 <sup>21</sup> [https://www.passportalmsp.com/blog/security-awareness-training-can-protect-](https://www.passportalmsp.com/blog/security-awareness-training-can-protect-against-phishing-attacks.)  
[against-phishing-attacks.](https://www.passportalmsp.com/blog/security-awareness-training-can-protect-against-phishing-attacks.)

1           68. Defendant is a multi-billion-dollar companies and has the resources  
2 necessary to prevent the Data Breach, but neglected to adequately invest in data security  
3 measures, despite its obligation to protect consumer data.

4           69. Had Defendant remedied the deficiencies in its data security systems and  
5 adopted security measures recommended by experts in the field, they would have  
6 prevented the intrusions into its systems and, ultimately, the theft of PII and PHI.

7           70. As a direct and proximate result of Defendant’ wrongful actions and  
8 inactions, Plaintiffs and Class Members have been placed at an imminent, immediate,  
9 and continuing increased risk of harm from identity theft and fraud, requiring them to  
10 take the time which they otherwise would have dedicated to other life demands such as  
11 work and family in an effort to mitigate the actual and potential impact of the Data Breach  
12 on their lives. The U.S. Department of Justice’s Bureau of Justice Statistics found that  
13 “among victims who had personal information used for fraudulent purposes, 29% spent  
14 a month or more resolving problems” and that “resolving the problems caused by identity  
15 theft [could] take more than a year for some victims.”<sup>22</sup>

16           71. The United States Government Accountability Office released a report in  
17 2007 regarding data breaches (“GOA Report”) in which it noted that victims of identity  
18 theft will face “substantial costs and time to repair the damage to their good name and  
19 credit record.”<sup>23</sup>

20           72. The FTC recommends that identity theft victims take several steps to  
21 protect their personal and financial information after a data breach, including contacting  
22 one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts  
23

---

24 <sup>22</sup> U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics,  
25 *Victims of Identity Theft*, 2012, December 2013 available at  
<https://www.bjs.gov/content/pub/pdf/vit12.pdf>

26 <sup>23</sup> See “Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is  
27 Limited; However, the Full Extent Is Unknown,” p. 2, U.S. Government Accountability  
28 Office, June 2007, <https://www.gao.gov/new.items/d07737.pdf> (last visited Apr. 12,  
2019) (“GAO Report”).

1 for 7 years if someone steals their identity), reviewing their credit reports, contacting  
2 companies to remove fraudulent charges from their accounts, placing a credit freeze on  
3 their credit, and correcting their credit reports.<sup>24</sup>

4 73. Identity thieves use stolen personal information such as Social Security  
5 numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and  
6 bank/finance fraud.

7 74. Identity thieves can also use Social Security numbers to obtain a driver's  
8 license or official identification card in the victim's name but with the thief's picture; use  
9 the victim's name and Social Security number to obtain government benefits; or file a  
10 fraudulent tax return using the victim's information. In addition, identity thieves may  
11 obtain a job using the victim's Social Security number, rent a house or receive medical  
12 services in the victim's name, and may even give the victim's personal information to  
13 police during an arrest resulting in an arrest warrant being issued in the victim's name. A  
14 study by Identity Theft Resource Center shows the multitude of harms caused by  
15 fraudulent use of personal and financial information:<sup>25</sup>

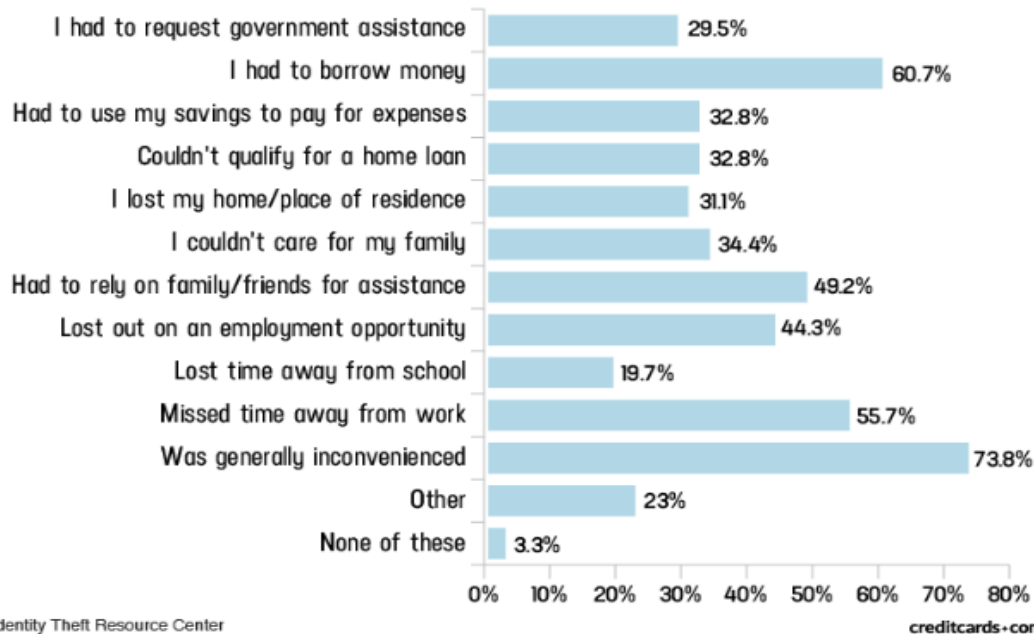
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26 

---

<sup>24</sup> See <https://www.identitytheft.gov/Steps> (last visited April 12, 2019).

27 <sup>25</sup> "Credit Card and ID Theft Statistics" by Jason Steele, 10/24/2017, at:  
28 <https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php> (last visited June 20, 2019).

## Americans' expenses/disruptions as a result of criminal activity in their name [2016]



75. What's more, PII constitutes a valuable property right, the theft of which is gravely serious.<sup>26</sup> Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

76. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs versus when it is discovered, and also between when PII and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years.

<sup>26</sup> See, e.g., John T. Soma, et al, Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“PII”) Equals the “Value” of Financial Assets, 15 Rich. J.L. & Tech. 11, at \*3-4 (2009) (“PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.”) (citations omitted).

1 As a result, studies that attempt to measure the harm resulting from  
2 data breaches cannot necessarily rule out all future harm.

3 *See* GAO Report, at p. 29.

4 77. PII and financial information are such valuable commodities to identity  
5 thieves that once the information has been compromised, criminals often trade the  
6 information on the “cyber black-market” for years.

7 78. There is a strong probability that entire batches of stolen information have  
8 been dumped on the black market and are yet to be dumped on the black market, meaning  
9 Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many  
10 years into the future. Thus, Plaintiffs and Class Members must vigilantly monitor their  
11 financial accounts for many years to come.

12 **L. PLAINTIFFS’ AND CLASS MEMBERS’ DAMAGES.**

13 79. To date, Defendant has merely offered identity theft and credit monitoring  
14 services at no charge for 36 months to the first tranche of persons notified of the breach,  
15 and offered no credit monitoring to those persons notified on June 12, 2020 or June 15,  
16 2020. Even if this credit monitoring was offered to all persons affected by this Data  
17 Breach, it is still wholly inadequate as it fails to provide for the fact that victims of data  
18 breaches and other unauthorized disclosures commonly face multiple years of ongoing  
19 identity theft and it entirely fails to provide any compensation for the unauthorized  
20 release and disclosure of Plaintiffs’ and Class Members’ PII and PIH.

21 80. Furthermore, Defendant’s credit monitoring offer to Plaintiffs and Class  
22 Members squarely places the burden on Plaintiffs and Class Members, rather than on the  
23 Defendant, to investigate and protect themselves from Defendant’s tortious acts resulting  
24 in the Data Breach. Rather than automatically enrolling Plaintiffs and Class Members in  
25 credit monitoring services upon discovery of the breach, Defendant’s merely sent  
26 instructions offering the services to affected employees, former employees, and their  
27 beneficiaries with the recommendation that they sign up for the services.  
28

1 81. Plaintiffs and Class Members have been damaged by the compromise of  
2 their PII and PHI in the Data Breach.

3 82. Plaintiffs' PII and PHI was compromised as a direct and proximate result  
4 of the Data Breach.

5 83. As a direct and proximate result of Defendant' conduct, Plaintiffs and Class  
6 Members have been placed at an imminent, immediate, and continuing increased risk of  
7 harm from fraud and identity theft.

8 84. As a direct and proximate result of Defendant's conduct, Plaintiffs and  
9 Class Members have been forced to expend time dealing with the effects of the Data  
10 Breach.

11 85. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud  
12 losses such as loans opened in their names, medical services billed in their names, tax  
13 return fraud, utility bills opened in their names, credit card fraud, and similar identity  
14 theft.

15 86. Plaintiffs and Class Members face substantial risk of being targeted for  
16 future phishing, data intrusion, and other illegal schemes based on their PII and PHI as  
17 potential fraudsters could use that information to more effectively target such schemes to  
18 Plaintiffs and Class Members.

19 87. Plaintiffs and Class Members may also incur out-of-pocket costs for  
20 protective measures such as credit monitoring fees, credit report fees, credit freeze fees,  
21 and similar costs directly or indirectly related to the Data Breach.

22 88. Plaintiffs and Class Members also suffered a loss of value of their PII and  
23 PHI when it was acquired by cyber thieves in the Data Breach. Numerous courts have  
24 recognized the propriety of loss of value damages in related cases.

25 89. Plaintiffs and Class Members have spent and will continue to spend  
26 significant amounts of time to monitor their financial accounts and records for misuse.

27 90. Plaintiffs and Class Members have suffered or will suffer actual injury as a  
28 direct result of the Data Breach. Many victims suffered ascertainable losses in the form

1 of out-of-pocket expenses and the value of their time reasonably incurred to remedy or  
2 mitigate the effects of the Data Breach relating to:

- 3 a. Finding fraudulent charges;
- 4 b. Canceling and reissuing credit and debit cards;
- 5 c. Purchasing credit monitoring and identity theft prevention;
- 6 d. Addressing their inability to withdraw funds linked to compromised  
7 accounts;
- 8 e. Taking trips to banks and waiting in line to obtain funds held in limited  
9 accounts;
- 10 f. Placing “freezes” and “alerts” with credit reporting agencies;
- 11 g. Spending time on the phone with or at a financial institution to dispute  
12 fraudulent charges;
- 13 h. Contacting financial institutions and closing or modifying financial  
14 accounts;
- 15 i. Resetting automatic billing and payment instructions from compromised  
16 credit and debit cards to new ones;
- 17 j. Paying late fees and declined payment fees imposed as a result of failed  
18 automatic payments that were tied to compromised cards that had to be  
19 cancelled; and
- 20 k. Closely reviewing and monitoring bank accounts and credit reports for  
21 unauthorized activity for years to come.

22 91. Moreover, Plaintiffs and Class Members have an interest in ensuring that  
23 their PII and PHI, which is believed to remain in the possession of Defendant, is protected  
24 from further breaches by the implementation of security measures and safeguards,  
25 including but not limited to, making sure that the storage of data or documents containing  
26 personal and financial information is not accessible online and that access to such data is  
27 password-protected.



1 92. Further, as a result of Defendant’s conduct, Plaintiffs and Class Members  
2 are forced to live with the anxiety that their PII and PHI—which contains the most  
3 intimate details about a person’s life —may be disclosed to the entire world, thereby  
4 subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

5 93. As a direct and proximate result of Defendant’ actions and inactions,  
6 Plaintiffs and Class Members have suffered anxiety, emotional distress, and loss of  
7 privacy, and are at an increased risk of future harm.

8 **V. CLASS ACTION ALLEGATIONS**

9 94. Plaintiffs bring this action on behalf of themselves and on behalf of all other  
10 persons similarly situated (“the Class”).

11 95. Plaintiffs propose the following Class definition, subject to amendment as  
12 appropriate:

13 All persons whose PII and PHI was compromised as a result of the  
14 Ransomware Attack that Magellan Health discovered on or about April 11,  
2020 (the “Class”).

15 96. Excluded from the Class are Defendant’s officers and directors, and any  
16 entity in which Defendant have a controlling interest; and the affiliates, legal  
17 representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also  
18 from the Class are Members of the judiciary to whom this case is assigned, their families  
19 and Members of their staff.

20 97. Plaintiffs hereby reserve the right to amend or modify the class definitions  
21 with greater specificity or division after having had an opportunity to conduct discovery.  
22 The proposed Class meets the criteria for certification under Rule 23(a), (b)(2), (b)(3) and  
23 (c)(4).

24 98. Numerosity. The Members of the Class are so numerous that joinder of all  
25 of them is impracticable. While the exact number of Class Members is unknown to  
26 Plaintiffs at this time, based on information and belief, the Class consists of  
27 approximately 163,654 employees, former employees, beneficiaries, and patients of  
28

1 Defendant Magellan Health and its affiliates named herein whose data was compromised  
2 in the Data Breach.

3 99. Commonality. There are questions of law and fact common to the Class,  
4 which predominate over any questions affecting only individual Class Members. These  
5 common questions of law and fact include, without limitation:

- 6 a. Whether Defendant unlawfully used, maintained, lost, or disclosed  
7 Plaintiffs' and Class Members' PII and PHI;
- 8 b. Whether Defendant 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 c. Whether Defendant' data security systems prior to and during the Data  
12 Breach complied with applicable data security laws and regulations;
- 13 d. Whether Defendant' data security systems prior to and during the Data  
14 Breach were consistent with industry standards;
- 15 e. Whether Defendant owed a duty to Class Members to safeguard their PII  
16 and PHI;
- 17 f. Whether Defendant breached its duty to Class Members to safeguard their  
18 PII and PHI;
- 19 g. Whether computer hackers obtained Class Members' PII and PHI in the  
20 Data Breach;
- 21 h. Whether Defendant knew or should have known that their data security  
22 systems and monitoring processes were deficient;
- 23 i. Whether Plaintiffs and Class Members suffered legally cognizable  
24 damages as a result of Defendant' misconduct;
- 25 j. Whether Defendant's conduct was negligent;
- 26 k. Whether Defendant' s conduct was per se negligent;
- 27 l. Whether Defendant's acts, inactions, and practices complained of herein  
28 amount to acts of intrusion upon seclusion under the law;

- 1 m. Whether Defendant was unjustly enriched;
- 2 n. Whether Defendant failed to provide notice of the Data Breach in a timely
- 3 manner, and;
- 4 o. Whether Plaintiffs and Class Members are entitled to damages, civil
- 5 penalties, punitive damages, and/or injunctive relief.

6 100. Typicality. Plaintiffs' claims are typical of those of other Class Members  
7 because Plaintiffs' PII and PHI, like that of every other Class member, was compromised  
8 in the Data Breach.

9 101. Adequacy of Representation. Plaintiffs will fairly and adequately represent  
10 and protect the interests of the Members of the Class. Plaintiffs' Counsel is competent  
11 and experienced in litigating Class actions, including data privacy litigation of this kind.

12 102. Predominance. Defendant have engaged in a common course of conduct  
13 toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data  
14 was stored on the same computer systems and unlawfully accessed in the same way. The  
15 common issues arising from Defendant's conduct affecting Class Members set out above  
16 predominate over any individualized issues. Adjudication of these common issues in a  
17 single action has important and desirable advantages of judicial economy.

18 103. Superiority. A Class action is superior to other available methods for the  
19 fair and efficient adjudication of the controversy. Class treatment of common questions  
20 of law and fact is superior to multiple individual actions or piecemeal litigation. Absent  
21 a Class action, most Class Members would likely find that the cost of litigating their  
22 individual claims is prohibitively high and would therefore have no effective remedy.  
23 The prosecution of separate actions by individual Class Members would create a risk of  
24 inconsistent or varying adjudications with respect to individual Class Members, which  
25 would establish incompatible standards of conduct for Defendant. In contrast, the conduct  
26 of this action as a Class action presents far fewer management difficulties, conserves  
27 judicial resources and the parties' resources, and protects the rights of each Class  
28 member.

1 104. Defendant has acted on grounds that apply generally to the Class as a  
2 whole, so that Class certification, injunctive relief, and corresponding declaratory relief  
3 are appropriate on a Class-wide basis.

4 105. Likewise, particular issues under Rule 23(c)(4) are appropriate for  
5 certification because such claims present only particular, common issues, the resolution  
6 of which would advance the disposition of this matter and the parties' interests therein.

7 Such particular issues include, but are not limited to:

- 8 a. Whether Defendant failed to timely notify the public of the Data Breach;
- 9 b. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise  
10 due care in collecting, storing, and safeguarding their PII and PHI;
- 11 c. Whether Defendant's security measures to protect their data systems were  
12 reasonable in light of best practices recommended by data security experts;
- 13 d. Whether Defendant's failure to institute adequate protective security  
14 measures amounted to negligence;
- 15 e. Whether Defendant failed to take commercially reasonable steps to  
16 safeguard consumer PII and PHI; and
- 17 f. Whether adherence to FTC data security recommendations, and measures  
18 recommended by data security experts would have reasonably prevented  
19 the data breach.

20 106. Finally, all members of the proposed Class are readily ascertainable.  
21 Defendant has access to Class Members' names and addresses affected by the Data  
22 Breach. Class Members have already been preliminarily identified and sent notice of the  
23 Data Breach by Defendant Magellan Health.

24 **VI. CAUSES OF ACTION**

25 **COUNT I**

26 **NEGLIGENCE**

27 **(On Behalf of Plaintiffs and All Class Members)**

1 107. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 106  
2 above as if fully set forth herein.

3 108. Defendant Magellan Health required Plaintiffs and Class Members to  
4 submit non-public PII as a condition of employment, or as a condition of receiving  
5 employee benefits, or as a condition of receiving medical or pharmaceutical care.

6 109. Plaintiffs and the Class Members entrusted their PII and PHI to Defendant  
7 with the understanding that Defendant would safeguard their information.

8 110. Defendant had full knowledge of the sensitivity of the PII and PHI and the  
9 types of harm that Plaintiffs and Class Members could and would suffer if the PII and  
10 PHI were wrongfully disclosed.

11 111. By assuming the responsibility to collect and store this data, and in fact  
12 doing so, and sharing it and using it for commercial gain, Defendant had a duty of care  
13 to use reasonable means to secure and safeguard their computer property—and Class  
14 Members' PII and PHI held within it—to prevent disclosure of the information, and to  
15 safeguard the information from theft. Defendant's duty included a responsibility to  
16 implement processes by which they could detect a breach of its security systems in a  
17 reasonably expeditious period of time and to give prompt notice to those affected in the  
18 case of a data breach.

19 112. Defendant had a duty to employ reasonable security measures under  
20 Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair  
21 . . . practices in or affecting commerce,” including, as interpreted and enforced by the  
22 FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

23 113. Defendant's duty of care to use reasonable security measures also arose as  
24 a result of the special relationship that existed between Defendant and its client patients,  
25 which is recognized by laws and regulations including but not limited to HIPAA, as well  
26 as common law. Defendant was in a position to ensure that its systems were sufficient to  
27 protect against the foreseeable risk of harm to Class Members from a data breach.

28

1 114. Defendant's duty to use reasonable security measures under HIPAA  
2 required Defendant to "reasonably protect" confidential data from "any intentional or  
3 unintentional use or disclosure" and to "have in place appropriate administrative,  
4 technical, and physical safeguards to protect the privacy of protected health information."  
5 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case  
6 constitutes "protected health information" within the meaning of HIPAA.

7 115. Defendant's duty to use reasonable care in protecting confidential data  
8 arose not only as a result of the statutes and regulations described above, but also because  
9 Defendant are bound by industry standards to protect confidential PII.

10 116. Defendant breached its duties, and thus was negligent, by failing to use  
11 reasonable measures to protect Class Members' PII and PHI. The specific negligent acts  
12 and omissions committed by Defendant include, but are not limited to, the following:

- 13 a. Failing to adopt, implement, and maintain adequate security measures to  
14 safeguard Class Members' PII and PHI;
- 15 b. Failing to adequately monitor the security of their networks and systems;
- 16 c. Failing to periodically ensure that their email system had plans in place to  
17 maintain reasonable data security safeguards;
- 18 d. Allowing unauthorized access to Class Members' PII and PHI;
- 19 e. Failing to detect in a timely manner that Class Members' PII and PHI had  
20 been compromised; and
- 21 f. Failing to timely notify Class Members about the Data Breach so that they  
22 could take appropriate steps to mitigate the potential for identity theft and  
23 other damages.

24 117. It was foreseeable that Defendant' failure to use reasonable measures to  
25 protect Class Members' PII and PHI would result in injury to Class Members. Further,  
26 the breach of security was reasonably foreseeable given the known high frequency of  
27 cyberattacks and data breaches in the data storage and healthcare industries.

1           118. It was therefore foreseeable that the failure to adequately safeguard Class  
2 Members' PII and PHI would result in one or more types of injuries to Class Members.

3           119. There is a temporal and close causal connection between Defendant' failure  
4 to implement security measures to protect the PII and PHI and the harm suffered, or risk  
5 of imminent harm suffered by Plaintiffs and the Class.

6           120. Plaintiffs and the Class Members had no ability to protect their PHI and PII  
7 that was in Defendant's possession.

8           121. Defendant was in a position to protect against the harm suffered by  
9 Plaintiffs and Class Members as a result of the Data Breach.

10           122. Defendant had a duty to put proper procedures in place in order to prevent  
11 the unauthorized dissemination of Plaintiffs' and Class Members' PHI and PII.

12           123. Defendant admitted that Plaintiffs' and Class Members' PII and PHI was  
13 wrongfully disclosed to unauthorized third persons as a result of the Data Breach.

14           124. As a result of Defendant's negligence, Plaintiffs and the Class Members  
15 have suffered and will continue to suffer damages and injury including, but not limited  
16 to: out-of-pocket expenses associated with procuring robust identity protection and  
17 restoration services; increased risk of future identity theft and fraud, the costs associated  
18 therewith; time spent monitoring, addressing and correcting the current and future  
19 consequences of the Data Breach; and the necessity to engage legal counsel and incur  
20 attorneys' fees, costs and expenses.

21           125. Plaintiffs and Class Members are entitled to compensatory and  
22 consequential damages suffered as a result of the Data Breach

23           126. Plaintiffs and Class Members are also entitled to injunctive relief requiring  
24 Defendant to, e.g., (i) strengthen their data security systems and monitoring procedures;  
25 (ii) submit to future annual audits of those systems and monitoring procedures; and (iii)  
26 continue to provide adequate credit monitoring to all Class Members.

**COUNT II**  
**NEGLIGENCE *PER SE***  
**(On Behalf of Plaintiffs and All Class Members)**

1  
2  
3 127. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 106  
4 above as if fully set forth herein.

5 128. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Defendant  
6 had a duty to provide fair and adequate computer systems and data security practices to  
7 safeguard Plaintiffs’ and Class Members’ PII and PHI.

8 129. Section 5 of the FTC Act prohibits “unfair . . . practices in or affecting  
9 commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice  
10 by businesses, such as Defendant’s, of failing to use reasonable measures to protect PII  
11 and PHI. The FTC publications and orders described above also form part of the basis of  
12 Defendant’s duty in this regard.

13 130. Defendant violated Section 5 of the FTC Act by failing to use reasonable  
14 measures to protect employee PII and PHI and not complying with applicable industry  
15 standards, as described in detail herein. Defendant’s conduct was particularly  
16 unreasonable given the nature and amount of PII and PHI it obtained and stored, and the  
17 foreseeable consequences of a data breach including, specifically, the damages that  
18 would result to Plaintiffs and Class Members.

19 131. Defendant’s violation of Section 5 of the FTC Act constitutes negligence  
20 per se as Defendant’s violation of the FTC Act establishes the duty and breach elements  
21 of negligence.

22 132. Plaintiffs and Class Members are within the class of persons that the FTC  
23 Act was intended to protect.

24 133. The harm that occurred as a result of the Data Breach is the type of harm  
25 the FTC Act was intended to guard against. The FTC has pursued enforcement actions  
26 against businesses, which, as a result of their failure to employ reasonable data security  
27 measures and avoid unfair and deceptive practices, caused the same harm as that suffered  
28 by Plaintiffs and the Class.



1 134. Pursuant to the Gramm-Leach-Bliley Act (15 U.S.C. § 6801), Defendant's  
2 had a duty to protect the security and confidentiality of Plaintiffs' and Class Members'  
3 PII.

4 135. Defendant breached its duties to Plaintiffs and Class Members under the  
5 Gramm-Leach-Bliley Act by failing to provide fair, reasonable, or adequate computer  
6 systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

7 136. Pursuant to HIPAA, 42 U.S.C. § 1302d, et seq., Defendant had a duty to  
8 implement reasonable safeguards to protect Plaintiffs' and Class Members' Private  
9 Information.

10 137. Pursuant to HIPAA, Defendant had a duty to render the electronic PHI it  
11 maintained unusable, unreadable, or indecipherable to unauthorized individuals, as  
12 specified in the HIPAA Security Rule by "the use of an algorithmic process to transform  
13 data into a form in which there is a low probability of assigning meaning without use of  
14 a confidential process or key." See definition of encryption at 45 C.F.R. § 164.304.

15 138. Defendant's failure to comply with applicable laws and regulations  
16 constitutes negligence per se.

17 139. But for Defendant's wrongful and negligent breach of its duties owed to  
18 Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

19 140. The injury and harm suffered by Plaintiffs and Class Members was the  
20 reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or  
21 should have known that it was failing to meet its duties, and that Defendant's breach  
22 would cause Plaintiffs and Class Members to experience the foreseeable harms associated  
23 with the exposure of their PII.

24 141. As a direct and proximate result of Defendant's negligent conduct,  
25 Plaintiffs and Class Members have suffered injury and are entitled to compensatory,  
26 consequential, and punitive damages in an amount to be proven at trial.

**COUNT III**  
**BREACH OF IMPLIED CONTRACT**  
**(On Behalf of Plaintiffs and all Class Members)**

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

142. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 106 above as if fully set forth herein.

143. Plaintiffs and Class Members were required to provide their PII and PHI to Defendant as a condition of their use of Defendant’s services, or as a condition of employment.

144. Plaintiffs and Class Members paid money to Defendant and disclosed their PII and PHI in exchange for medical and pharmaceutical services, along with Defendant’s promise to protect their PII and PHI from unauthorized disclosure.

145. Plaintiffs also provided their labor and employee services to Defendant, as well as turning over their PII to Defendant, in exchange for Defendant’s promise to protect their PII from unauthorized disclosure.

146. In its written privacy policies, Defendant Magellan Health expressly promised Plaintiffs and Class Members that it would only disclose PII or PHI under certain circumstances, none of which relate to the Data Breach.

147. Defendant further promised to comply with industry standards and to make sure that Plaintiffs’ and Class Members’ PII and PHI would remain protected.

148. Implicit in the agreement between Plaintiffs and Class Members and the Defendant to provide PII, was the latter’s obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiffs and Class Members from unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such information secure and confidential.

1           149. When Plaintiffs and Class Members provided their PII to Defendant  
2 Magellan Health as a condition of their employment or employee beneficiary status, or  
3 as a condition precedent to receiving medical or pharmaceutical care, they entered into  
4 implied contracts with Defendant pursuant to which Defendant agreed to reasonably  
5 protect such information.

6           150. Defendant solicited, invited, and then required Class Members to provide  
7 their PII and PHI as part of Defendant's regular business practices. Plaintiffs and Class  
8 Members accepted Defendant's offers and provided their PII to Defendant.

9           151. In entering into such implied contracts, Plaintiffs and Class Members  
10 reasonably believed and expected that Defendant's data security practices complied with  
11 relevant laws and regulations and were consistent with industry standards.

12           152. Plaintiffs and Class Members would not have entrusted their PII to  
13 Defendant in the absence of the implied contract between them and Defendant to keep  
14 their information reasonably secure. Plaintiffs and Class Members would not have  
15 entrusted their PII to Defendant in the absence of its implied promise to monitor its  
16 computer systems and networks to ensure that it adopted reasonable data security  
17 measures.

18           153. Plaintiffs and Class Members fully and adequately performed their  
19 obligations under the implied contracts with Defendant.

20           154. Defendant breached their implied contracts with Class Members by failing  
21 to safeguard and protect their PII and PHI.

22           155. As a direct and proximate result of Defendant's breaches of the implied  
23 contracts, Class Members sustained damages as alleged herein.

24           156. Plaintiffs and Class Members are entitled to compensatory and  
25 consequential damages suffered as a result of the Data Breach.

26           157. Plaintiffs and Class Members are also entitled to injunctive relief requiring  
27 Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii)  
28

1 submit to future annual audits of those systems and monitoring procedures; and (iii)  
2 immediately provide adequate credit monitoring to all Class Members.

3 **COUNT IV**  
4 **UNJUST ENRICHMENT**  
5 **(On Behalf of Plaintiffs and All Class Members)**

6 158. Plaintiffs restate and reallege paragraphs 1 through 106 above as if fully set  
7 forth herein.

8 159. Plaintiffs and Class Members conferred a monetary benefit on Defendant.  
9 Specifically, Defendant enriched itself by saving the costs it reasonably should have  
10 expended on data security measures to secure Plaintiffs' and Class Members' Personal  
11 Information. Instead of providing a reasonable level of security that would have  
12 prevented the Data Breach, Defendant instead calculated to increase its own profits at the  
13 expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security  
14 measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and  
15 proximate result of Defendant' decision to prioritize its own profits over the requisite  
16 security.

17 160. Under the principles of equity and good conscience, Defendant should not  
18 be permitted to retain the money belonging to Plaintiffs and Class Members, because  
19 Defendant failed to implement appropriate data management and security measures that  
20 are mandated by industry standards.

21 161. Defendant acquired the PII through inequitable means in that it failed to  
22 disclose the inadequate security practices previously alleged.

23 162. If Plaintiffs and Class Members knew that Defendant had not secured their  
24 PII, they would not have agreed to provide their PII to Defendant Magellan Health.

25 163. Plaintiffs and Class Members have no adequate remedy at law.

26 164. As a direct and proximate result of Defendant's conduct, Plaintiffs and  
27 Class Members have suffered and will suffer injury, including but not limited to: (i) actual  
28 identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise,  
publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with

1 the prevention, detection, and recovery from identity theft, and/or unauthorized use of  
2 their PII and PHI; (v) lost opportunity costs associated with effort expended and the loss  
3 of productivity addressing and attempting to mitigate the actual and future consequences  
4 of the Data Breach, including but not limited to efforts spent researching how to prevent,  
5 detect, contest, and recover from identity theft; (vi) the continued risk to their PII and  
6 PHI, which remain in Defendant's possession and is subject to further unauthorized  
7 disclosures so long as Defendant fails to undertake appropriate and adequate measures to  
8 protect PII and PHI in its continued possession; and (vii) future costs in terms of time,  
9 effort, and money that will be expended to prevent, detect, contest, and repair the impact  
10 of the PII and PHI compromised as a result of the Data Breach for the remainder of the  
11 lives of Plaintiffs and Class Members.

12 165. As a direct and proximate result of Defendant's conduct, Plaintiffs and  
13 Class Members have suffered and will continue to suffer other forms of injury and/or  
14 harm.

15 166. Defendant should be compelled to disgorge into a common fund or  
16 constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they  
17 unjustly received from them. In the alternative, Defendant should be compelled to refund  
18 the amounts that Plaintiffs and Class Members overpaid for Defendant's services.

19 **COUNT V**  
20 **ARIZONA CONSUMER FRAUD ACT ("ACFA")**  
21 **Ariz. Rev. Stat. §§ 44-1521, et seq.**

22 167. Plaintiffs restate and reallege paragraphs 1 through 106 as if fully set forth  
23 herein.

24 168. The ACFA provides in pertinent part: "The act, use or employment by any  
25 person of any deception, deceptive or unfair act or practice, fraud, false pretense, false  
26 promise, misrepresentation, or concealment, suppression or omission of any material fact  
27 with intent that others rely on such concealment, suppression or omission, in connection  
28 with the sale or advertisement of any merchandise whether or not any person has in face

1 been misled, deceived or damaged thereby, is declared to be an unlawful practice.” Ariz.  
2 Rev. Stat. § 44-1522.

3 169. Plaintiffs and Class Members are “persons” as defined by Ariz. Rev. Stat.  
4 § 44-1521(6).

5 170. Defendant Magellan Health provides “services” as that term is included in  
6 the definition of “merchandise” under Ariz. Rev. Stat. § 44-1521(5), and Defendant is  
7 engaged in the “sale” of “merchandise” as defined by Ariz. Rev. Stat. § 44-1521(7).

8 171. Defendant engaged in deceptive and unfair acts and practices,  
9 misrepresentation, and the concealment, suppression and omission of material facts in  
10 connection with the sale and advertisement of “merchandise” (as defined in the ACFA)  
11 in violation of the ACFA, including but not limited to the following:

- 12 a. Failing to maintain sufficient security to keep Plaintiffs’ and Class  
13 Members’ confidential medical, financial and personal data from being  
14 hacked and stolen;
- 15 b. Failing to disclose the Data Breach to Class Members in a timely and  
16 accurate manner, in violation of Ariz. Rev. Stat. § 18-552(B);
- 17 c. Misrepresenting material facts, pertaining to the sale of health benefit  
18 services by representing that they would maintain adequate data privacy  
19 and security practices and procedures to safeguard Class Members’ PHI  
20 and PII from unauthorized disclosure, release, data breaches, and theft;
- 21 d. Misrepresenting material facts, in connection with the sale of health benefit  
22 services by representing that they did and would comply with the  
23 requirements of relevant federal and state laws pertaining to the privacy  
24 and security of Class Members’ PHI and PII;
- 25 e. Omitting, suppressing, and concealing the material fact of the inadequacy  
26 of the data privacy and security protections for Class Members’ PHI and  
27 PII;

- 1 f. Engaging in unfair, unlawful, and deceptive acts and practices with respect  
2 to the sale of health benefit services by failing to maintain the privacy and  
3 security of Class Members' PHI and PII, in violation of duties imposed by  
4 and public policies reflected in applicable federal and state laws, resulting  
5 in the Data Breach. These unfair, unlawful, and deceptive acts and practices  
6 violated duties imposed by laws, including HIPAA and Section 5 of the  
7 FTC Act;
- 8 g. Engaging in unlawful, unfair, and deceptive acts and practices with respect  
9 to the sale of health benefit services by failing to disclose the Data Breach  
10 to Class Members in a timely and accurate manner;
- 11 h. Engaging in unlawful, unfair, and deceptive acts and practices with respect  
12 to the sale of health benefit services by failing to take proper action  
13 following the Data Breach to enact adequate privacy and security measures  
14 and protect Class Members' PHI and PII from further unauthorized  
15 disclosure, release, data breaches, and theft.

16 172. The above unlawful, unfair, and deceptive acts and practices by Magellan  
17 were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial  
18 injury to Plaintiffs and Class Members that they could not reasonably avoid; this  
19 substantial injury outweighed any benefits to consumers or to competition.

20 173. Defendant knew or should have known that their computer systems and  
21 data security practices were inadequate to safeguard Class Members' PHI and PII and  
22 that risk of a data breach or theft was high, as Defendant was the subject of another similar  
23 phishing attack that resulted in a data breach in May 2019. Magellan's actions in  
24 engaging in the above-named deceptive acts and practices were negligent, knowing and  
25 willful, and/or wanton and reckless with respect to the rights of Members of the Class.

26 174. As a direct and proximate result of Defendant's deceptive acts and  
27 practices, the Class Members suffered an ascertainable loss of money or property, real or  
28

1 personal, as described above, including the loss of their legally protected interest in the  
2 confidentiality and privacy of their PHI and PII.

3 175. Plaintiffs and Class Members seek relief under the ACFA including, but  
4 not limited to, injunctive relief, actual damages, treble damages for each willful or  
5 knowing violation, and attorneys' fees and costs.

6 **PRAYER FOR RELIEF**

7 WHEREFORE, Plaintiffs, individually and on behalf of the Class, respectfully  
8 request that the Court award the following on all counts:

- 9 A. For an Order certifying this action as a Class action and appointing Plaintiffs  
10 and their counsel to represent the Class;
- 11 B. For equitable relief enjoining Defendant from engaging in the wrongful  
12 conduct complained of herein pertaining to the misuse and/or disclosure of  
13 Plaintiffs' and Class Members' PII, and from refusing to issue prompt,  
14 complete and accurate disclosures to Plaintiffs and Class Members;
- 15 C. For equitable relief compelling Defendant to utilize appropriate methods and  
16 policies with respect to consumer data collection, storage, and safety, and to  
17 disclose with specificity the type of PII compromised during the Data Breach;
- 18 D. For equitable relief requiring restitution and disgorgement of the revenues  
19 wrongfully retained as a result of Defendant's wrongful conduct;
- 20 E. Ordering Defendant to pay for not less than seven years of credit monitoring  
21 services for Plaintiffs and the Class;
- 22 F. For an award of actual damages, compensatory damages, statutory damages,  
23 and statutory penalties, in an amount to be determined, as allowable by law;
- 24 G. For an award of punitive damages, as allowable by law;
- 25 H. For an award of attorneys' fees and costs, and any other expense, including  
26 expert witness fees;
- 27 I. Pre- and post-judgment interest on any amounts awarded; and
- 28 J. Such other and further relief as this court may deem just and proper.



**DEMAND FOR JURY TRIAL**

Plaintiffs, individually and on behalf of the Class, demand a trial by jury on all issues so triable.

Dated: June 29, 2020

Respectfully submitted,

**ZIMMERMAN REED LLP**

By: s/ Hart L. Robinovitch  
Hart L. Robinovitch (AZ SBN 020910)  
14646 North Kierland Blvd., Suite 145  
Scottsdale, AZ 85254  
Telephone: (480) 348-6400  
Facsimile: (480) 348-6415  
Email: hart.robinovitch@zimmreed.com

**MASON LIETZ & KLINGER LLP**  
Gary E. Mason (*Pro Hac Vice* to be filed)  
David K. Lietz (*Pro Hac Vice* to be filed)  
5301 Wisconsin Ave, NW  
Suite 305  
Washington, DC 20016  
Telephone: (202) 429-2290  
Facsimile:  
Email: gmason@masonllp.com  
Email: dlietz@masonllp.com

**MASON LIETZ & KLINGER LLP**  
Gary M. Klinger (*Pro Hac Vice* to be filed)  
227 W. Monroe Street, Suite 2100  
Chicago, IL 60630  
Telephone: (312) 283-3814  
Facsimile:  
Email: gklinger@masonllp.com

*Attorneys for Plaintiffs*

# EXHIBIT A



Return Mail Processing  
PO Box 589  
Claysburg, PA 16625-0589

May 12, 2020



F5229-L01-0014194 P003 T00043 ALL FOR AADC 370  
BHARATH MADURANTHAGAM RAYAM  
407 BRENTWOOD OAKS DR  
NASHVILLE TN 37211-6526



Dear Bharath Rayam:

Magellan was recently the victim of a criminal ransomware attack. We are writing to let you know how this incident may have affected your personal information and, as a precaution, to provide steps you can take to help protect your information. We take the privacy and security of your personal information very seriously and we sincerely regret any concern this incident may cause you.

***What Happened***

On April 11, 2020, Magellan discovered it was targeted by a ransomware attack. The unauthorized actor gained access to Magellan's systems after sending a phishing email on April 6 that impersonated a Magellan client. Once the incident was discovered, Magellan immediately retained a leading cybersecurity forensics firm, Mandiant, to help conduct a thorough investigation of the incident. The investigation revealed that prior to the launch of the ransomware, the unauthorized actor exfiltrated a subset of data from a single Magellan corporate server, which included some of your personal information. In limited instances, and only with respect to certain current employees, the unauthorized actor also used a piece of malware designed to steal login credentials and passwords. At this point, we are not aware of any fraud or misuse of any of your personal information as a result of this incident, but we are notifying you out of an abundance of caution.

***What Information Was Involved***

The exfiltrated records include personal information such as name, address, employee ID number, and W-2 or 1099 details such as Social Security number or Taxpayer ID number and, in limited circumstances, may also include usernames and passwords.

***What We Are Doing***

Magellan immediately reported the incident to, and is working closely with, the appropriate law enforcement authorities, including the FBI. Additionally, to help prevent a similar type of incident from occurring in the future, we implemented additional security protocols designed to protect our network, email environment, systems, and personal information.

8621 Robert Fulton Drive, Columbia, MD 21046  
[www.magellanhealth.com](http://www.magellanhealth.com)



F5229-L01

### Information About Identity Theft Protection Guide

Contact information for the three nationwide credit reporting companies is as follows:

Equifax	Experian	TransUnion
Phone: 1-800-685-1111 P.O. Box 740256 Atlanta, Georgia 30348 www.equifax.com	Phone: 1-888-397-3742 P.O. Box 9554 Allen, Texas 75013 www.experian.com	Phone: 1-888-909-8872 P.O. Box 105281 Atlanta, GA 30348-5281 www.transunion.com

**Free Credit Report.** We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at [www.consumer.ftc.gov](http://www.consumer.ftc.gov)) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

**For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:**

You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

**Security Freeze.** Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

Don't confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

**For New Mexico residents:** You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.





**EXHIBIT B**



Return Mail Processing  
PO Box 589  
Claysburg, PA 16625-0589

May 15, 2020



F5300-L01-0030277 P003 T00074 \*\*\*\*\*ALL FOR AADC 630  
CHRIS A GRIFFEY  
2328 DARTMOUTH BEND DR  
WILDWOOD, MO 63011-5426



Dear Chris A Griffey:

Magellan was recently the victim of a criminal ransomware attack. We are writing to let you know how this incident may have affected your personal information and, as a precaution, to provide steps you can take to help protect your information. We take the privacy and security of your personal information very seriously and we sincerely regret any concern this incident may cause you.

### ***What Happened***

On April 11, 2020, Magellan discovered it was targeted by a ransomware attack. The unauthorized actor gained access to Magellan's systems after sending a phishing email on April 6 that impersonated a Magellan client. Once the incident was discovered, Magellan immediately retained a leading cybersecurity forensics firm, Mandiant, to help conduct a thorough investigation of the incident. The investigation revealed that prior to the launch of the ransomware, the unauthorized actor exfiltrated a subset of data from a single Magellan corporate server, which included some of your personal information. In limited instances, and only with respect to certain current employees, the unauthorized actor also used a piece of malware designed to steal login credentials and passwords. At this point, we are not aware of any fraud or misuse of any of your personal information as a result of this incident, but we are notifying you out of an abundance of caution.

### ***What Information Was Involved***

The exfiltrated records include personal information such as name, address, employee ID number, and W-2 or 1099 details such as Social Security number or Taxpayer ID number and, in limited circumstances, may also include usernames and passwords.

### ***What We Are Doing***

Magellan immediately reported the incident to, and is working closely with, the appropriate law enforcement authorities, including the FBI. Additionally, to help prevent a similar type of incident from occurring in the future, we implemented additional security protocols designed to protect our network, email environment, systems, and personal information.

8621 Robert Fulton Drive, Columbia, MD 21046  
[www.magellanhealth.com](http://www.magellanhealth.com)

0030277



F5300-L01

***What You Can Do***

Please review the "Information About Identity Theft Protection" reference guide, enclosed here, which describes additional steps you may take to help protect yourself, including recommendations from the Federal Trade Commission regarding identity theft protection and details regarding placing a fraud alert or a security freeze on your credit file. As an added precaution, to help protect your identity, we are offering a complimentary three-year membership of Experian's® IdentityWorks<sup>SM</sup>. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

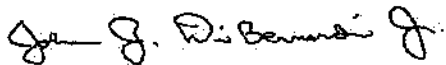
- Ensure that you enroll by: August 31, 2020 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your activation code: 5TVD5BX3V

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 855-252-3244 by August 31, 2020. Be prepared to provide engagement number DB19941 as proof of eligibility for the identity restoration services by Experian.

***For More Information***

The security of your personal information is important to us and we sincerely regret that this incident occurred. For more information, or if you have any questions or need additional information, please contact 855-252-3244.

Sincerely,



John J. DiBernardi Jr., Esq.  
Senior Vice President & Chief Compliance Officer

**For Colorado and Illinois residents:** You may obtain information from the credit reporting agencies and the FTC about security freezes.

**Fraud Alerts.** A fraud alert tells businesses that check your credit that they should check with you before opening a new account. As of September 18, 2018 when you place a fraud alert, it will last one year, instead of 90 days. Fraud alerts will still be free and identity theft victims can still get an extended fraud alert for seven years.

**For Colorado and Illinois residents:** You may obtain additional information from the credit reporting agencies and the FTC about fraud alerts.

**Federal Trade Commission and State Attorneys General Offices.** If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, [www.ftc.gov/bcp/edu/microsites/idtheft/](http://www.ftc.gov/bcp/edu/microsites/idtheft/), 1-877-IDTHEFT (438-4338).

**For Maryland Residents:** You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, [www.oag.state.md.us](http://www.oag.state.md.us), 1-888-743-0023.

**For North Carolina residents:** You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, [www.ncdoj.gov](http://www.ncdoj.gov), 1-877-566-7226.

**For Rhode Island Residents:** You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, <http://www.riag.ri.gov>, 401-274-4400.

**Reporting of identity theft and obtaining a police report.**

You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

**For Iowa residents:** You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

**For Massachusetts residents:** You have the right to obtain a police report if you are a victim of identity theft. You also have a right to file a police report and obtain a copy of it.

**For Oregon residents:** You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

**For Rhode Island residents:** You have the right to file or obtain a police report regarding this incident.





**Information About Identity Theft Protection Guide**

Contact information for the three nationwide credit reporting companies is as follows:

<b>Equifax</b>	<b>Experian</b>	<b>TransUnion</b>
Phone: 1-800-685-1111 P.O. Box 740256 Atlanta, Georgia 30348 www.equifax.com	Phone: 1-888-397-3742 P.O. Box 9554 Allen, Texas 75013 www.experian.com	Phone: 1-888-909-8872 P.O. Box 105281 Atlanta, GA 30348-5281 www.transunion.com

**Free Credit Report.** We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at [www.consumer.ftc.gov](http://www.consumer.ftc.gov)) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

**For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:**

You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

**Security Freeze.** Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

Don't confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display the name and complete mailing address, and the date of issue.

**New Mexico residents:** You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Credit Reporting and Identity Security Act.



# EXHIBIT C

**From:** [Michael Domingo](#)  
**To:** [Domingo, Michael](#)  
**Subject:** Fwd: Security Incident Notification  
**Date:** Tuesday, June 23, 2020 3:00:08 PM

---

**EXTERNAL EMAIL** – Use caution with any links or file attachments.

----- Forwarded message -----

**From:** Security Incident Notification <[Incident@magellanhealth.com](mailto:Incident@magellanhealth.com)>  
**Date:** Mon, May 4, 2020 at 3:03 PM  
**Subject:** Security Incident Notification  
**To:** <[michael.p.domingo22@gmail.com](mailto:michael.p.domingo22@gmail.com)>

*This email was sent to all former Magellan employees on Monday, May 4 to provide preliminary notification of W-2 information exfiltration.*

Is this email not displaying correctly?  
[View it in your browser.](#)



Dear Former Magellan Health Employee:

At Magellan Health, we take privacy and information security very seriously, which is why we want to share with you some information regarding a recent ransomware attack against the company.

While we have been remediating and investigating this attack, we recently learned that the threat actor responsible for this ransomware attack on Magellan also stole documents containing W-2 information for all Magellan Health employees who were employed in 2019, which includes Social Security numbers.

It is important to note we have no reason to believe any of your information has been used inappropriately. In fact, we do not believe your W-2 information was targeted by the threat actor for identity theft purposes, but rather, such information happened to be included in documents taken by the threat actor as part of the ransomware attack. Nonetheless, we wanted to inform you about this immediately, so you could take steps to protect yourself in an abundance of caution.

To that end, we are offering you free identity theft monitoring services through Experian. This service will include free credit monitoring from the three national credit bureaus and identity restoration services. We are also contacting the IRS to inform them of the W-2 theft so that they can monitor tax filings.

In the coming days you will receive a letter from Experian, which will provide further details on the situation. This letter will also include information on the steps you can take, including how to set up the identity protection services being offered to you at no cost to help protect you from potential identity theft, as well as additional precautionary measures you can take.

If you wish to take any immediate precautionary action before receiving our offered identity theft monitoring services, you may place a fraud alert or credit freeze on your credit file through any of the three credit bureaus and receive a credit report for your review free of charge:

- Equifax: [Equifax.com](https://www.equifax.com) or 1-800-685-1111
- Experian: [Experian.com](https://www.experian.com) or 1-888-397-3742
- TransUnion: [TransUnion.com](https://www.transunion.com) or 1-888-909-8872

We apologize for any inconvenience this matter might cause you and thank you for your patience and understanding while we work through this issue.

John DiBernardi  
Chief Compliance Officer

----

## Former Employee Q&A

### **Exactly what was stolen and how did it happen?**

Magellan Health was the victim of a recent ransomware attack on our Company. While we have contained the incident, our investigation into the incident, supported by third-party experts and law enforcement, continues.

We recently learned W-2 information for all Magellan Health employees in 2019, which includes Social Security numbers and home addresses, was stolen. We have no reason to believe your information has been used inappropriately.

### **I no longer work for Magellan Health, how was I impacted?**

Information impacted by this incident includes W-2 information for all Magellan Health employees in 2019.

### **How many Magellan employees were impacted?**

Information impacted by this incident includes W-2 information for all Magellan Health employees in 2019.

### **How was my information (SSN) stolen?**

We have been in the process of conducting a thorough forensic review of the recent cybersecurity incident and have confirmed your employee pay information was impacted by a data exfiltration. This information was included on W-2 forms, which includes Social Security numbers and home addresses.

### **Was my identity stolen? If not, how will I know if my data is being used?**

We have no reason to believe your information has been used inappropriately.

In the coming days, you will receive a letter from Experian, which will provide further details on the situation. This letter will include information on the steps you can take, including how to set up the identity protection services being offered to you at no cost to help protect you from potential identity theft, as well as additional precautionary measures you can take.

If you wish to take any immediate precautionary action before receiving our offered identity theft monitoring services, you may place a fraud alert or credit freeze on your credit file through any of the three credit bureaus and receive a credit report for your review free of charge:

- Equifax: [Equifax.com](https://www.equifax.com) or 1-800-685-1111
- Experian: [Experian.com](https://www.experian.com) or 1-888-397-3742
- TransUnion: [TransUnion.com](https://www.transunion.com) or 1-888-909-8872

**What are you doing to protect my financial data?**

We have no reason to believe your financial data has been used inappropriately. We are offering you free identity theft monitoring service through Experian. You will receive details on this service in the coming days in a mailed letter from Experian.

The offered service at no cost to you will include free credit monitoring from the three national credit bureaus and identity restoration services. We are also contacting the IRS to inform them of the W-2 theft so that they can monitor tax filings.

**What should I do to protect my financial data?**

We have no reason to believe your financial data has been used inappropriately.

In the coming days you will receive a letter from Experian, which will provide further details on the situation. This letter will also include information on the steps you can take, including how to set up the identity protection services being offered to you at no cost to help protect you from potential identity theft, as well as additional precautionary measures you can take.

If you wish to take any immediate precautionary action before receiving our offered identity theft monitoring services, you may place a fraud alert or credit freeze on your credit file through any of the three credit bureaus and receive a credit report for your review free of charge:

- Equifax: [Equifax.com](https://www.equifax.com) or 1-800-685-1111
- Experian: [Experian.com](https://www.experian.com) or 1-888-397-3742
- TransUnion: [TransUnion.com](https://www.transunion.com) or 1-888-909-8872

**Is my financial information being sold?**

We have no reason to believe your information has been used inappropriately.

**If my data is not being sold, how else could a criminal use my data?**

We have no reason to believe your information has been used inappropriately. If you believe your

personal information has been misused, visit the FTC's site at [IdentityTheft.gov](https://www.ftc.gov/identity-theft) to get recovery steps and to file an identity theft complaint. Your complaint will be added to the FTC's Consumer Sentinel Network, where it will be accessible to law enforcers for their investigations.

### Should I contact the IRS?

If you suspect you are a victim of tax-related identity theft, the IRS recommends taking the following steps:

- If you received an [IRS 5071C](#) or an [IRS 5747C](#) letter; call the number provided in the notice or, if instructed, visit the IRS's Identity Verification Service at [https://go.magellanhealth.com/e/703943/ud-scams-identity-verification/hbglz/100020545?h=ziA8fPKAtJXJjxjkKcGqn62ScaQZf\\_nN85sloy9fJyl](https://go.magellanhealth.com/e/703943/ud-scams-identity-verification/hbglz/100020545?h=ziA8fPKAtJXJjxjkKcGqn62ScaQZf_nN85sloy9fJyl).
- Complete IRS Form 14039, Identity Theft Affidavit, if your e-filed return is rejected because of a duplicate filing under your SSN or you are otherwise instructed to do so.

### Is this going to impact my 2019 tax return or my COVID-19 Economic Impact Payment?

No, we have no reason to believe that your information has been used inappropriately.

If you suspect you are a victim of tax-related identity theft, the IRS recommends taking the following steps:

- If instructed, visit the IRS's Identity Verification Service at [https://go.magellanhealth.com/e/703943/ud-scams-identity-verification/hbglz/100020545?h=ziA8fPKAtJXJjxjkKcGqn62ScaQZf\\_nN85sloy9fJyl](https://go.magellanhealth.com/e/703943/ud-scams-identity-verification/hbglz/100020545?h=ziA8fPKAtJXJjxjkKcGqn62ScaQZf_nN85sloy9fJyl).
- Complete IRS Form 14039, Identity Theft Affidavit, if your e-filed return is rejected because of a duplicate filing under your SSN or you are otherwise instructed to do so.

### What will Magellan Health do if I am financially impacted by this? Will I be reimbursed?

When the Experian letter arrives, we encourage you to sign up for identity theft protection services, which includes insurance for fraud and identity theft.

### Where can I learn more information?

In the coming days you will receive an official notification letter from our identity theft monitoring vendor partner, Experian. This notification letter will provide further details on the situation, including what is being offered to you to help protect you from potential identity theft and what additional precautionary measures you can take.

© 2020 Magellan Health, Inc.

This email was sent by Magellan Health:  
4801 East Washington Street  
Phoenix, AZ 85034



<https://go.magellanhealth.com/unsubscribe/u/703943/c2af7624b18b5e77141bfd88d826f6724d55ba02e0da5165a96f4a241fed264a/100020545>

