# Exhibit A1

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

*Attorneys for Plaintiffs and the Class*

*(Additional Counsel listed below)*

**UNITED STATES DISTRICT COURT**

**DISTRICT OF ARIZONA**

| | |
|---|---|
| Chris Griffey, Bharath Maduranthgam Rayam, Michael Domingo, and Laura Leather individually and on behalf of all others similarly situated,<br><br>Plaintiffs,<br><br>-v-<br><br>Magellan Health, Inc., a Delaware corporation,<br><br>Defendant. | Case No. CV-20-1282-PHX-MTL<br><br>**FIRST AMENDED CLASS ACTION COMPLAINT**<br><br>**DEMAND FOR JURY TRIAL** |

Plaintiffs CHRIS GRIFFEY, BHARATH MADURANTHGAM RAYAM, MICHAEL DOMINGO, and LAURA LEATHER ("Plaintiffs"), individually, and on behalf of all others similarly situated, bring this action against Defendant, MAGELLAN HEALTH, INC. to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and the facts that are a matter of public record:

## I. PARTIES

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

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

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

4. Plaintiff LAURA LEATHER is, and at all times mentioned herein was, an individual citizen of the state of New York residing in the city of Dover Plains. Upon information and belief, Magellan Health provided services to her employer or to her health plan. Plaintiff Leather received notice of the data breach, and a copy of the notice is attached hereto as Exhibit D. As a result of the data breach, Leather has taken

responsive measures that she otherwise would not have taken to ensure that her identity is not stolen and that her personal affairs are not further compromised.

5. Defendant Magellan Health ("Magellan Health, Inc." or "Defendant") is a publicly traded Delaware corporation headquartered at 4801 E. Washington Street, Phoenix, Arizona 85034. It is a Fortune 500 company broadly operating in the healthcare management business.

## II. JURISDICTION

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

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

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

## III. NATURE OF THE ACTION

9. This class action arises out of the most recent targeted cyberattack and data breach ("Data Breach") involving Magellan Health, Inc. and its subsidiaries and affiliates

(collectively, "Magellan Health").[1] As a result of the Data Breach, the PII and PHI of Plaintiffs and at least 365,000 Class members is in the hands of cyberthieves. Plaintiffs and Class Members suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack. In addition, Plaintiffs' and Class members' sensitive personal information—which was entrusted to Magellan Health, its officials and agents—was compromised and unlawfully accessed due to the Data Breach. Information compromised in the Data Breach included names, contact information, employee ID numbers, and W-2 or 1099 information, including Social Security numbers or taxpayer identification numbers, treatment information, health insurance account information, member IDs, other health-related information, email addresses, phone numbers, physical addresses, and additional PII.

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

11. Defendant maintained the PII and PHI in a reckless manner. In particular, the PII and PHI was maintained on Defendant Magellan Health's computer network in a condition vulnerable to cyberattacks. The mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class members' PII and PHI was a known risk to Defendant, as it was subject to another data breach a mere 11 months prior that

[1] Magellan Health, Inc.'s affiliates involved in the breach include but are not limited to: Magellan Healthcare, Inc. (55,637 patients), Merit Health Insurance Company (102,748 patients), Florida MHS, Inc. d/b/a Magellan Complete Care of Florida (76,236 patients), the University of Florida Health Jacksonville (54,002 patients), Magellan Healthcare of Maryland, LLC (50,410 patients), VRx Pharmacy (33,040 patients), National Imaging Associates, Inc. (22,560 patients), UF Health Shands (13,146 patients), UF Health (9,182 patients), and Magellan Complete Care of Virginia, LLC (3,568 patients).

involved another phishing attack, and thus Defendant was on notice that failing to take steps necessary to secure the PII and PHI from those risks left that property in a dangerous condition.

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

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

14. Armed with the PII and PHI accessed in the Data Breach, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in Class members' names, taking out loans in Class members' names, using Class members' names to obtain medical services, using Class members' health information to target other phishing and hacking intrusions based on their individual health needs, using Class members' information to obtain government benefits, filing fraudulent tax returns using Class members' information, obtaining driver's licenses in Class members' names, but with another person's photograph, and giving false information to police during an arrest.

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

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

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

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

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

## IV. STATEMENT OF FACTS

### A. Defendant Magellan Health.

20. Defendant Magellan Health is a for-profit managed health care company, focused on special populations, complete pharmacy benefits and other specialty areas of healthcare. It directly manages health benefits for its members' patients, including those of its affiliates/subsidiaries Magellan Healthcare, Inc. (55,637 patients); Merit Health Insurance Company (102,748 patients), Florida MHS, Inc. d/b/a Magellan Complete Care of Florida (76,236 patients), the University of Florida Health Jacksonville (54,002 patients), Magellan Healthcare of Maryland, LLC (50,410 patients), VRx Pharmacy (33,040 patients), National Imaging Associates, Inc. (22,560 patients), UF Health Shands (13,146 patients), UF Health (9,182 patients), and Magellan Complete Care of Virginia, LLC (3,568 patients).

21. As part of its contractual relationship with the aforementioned affiliates/subsidiaries and several other providers, Defendant administers the health and pharmaceutical benefits offered by those affiliates/subsidiaries. Defendant Magellan Health received fees from these affiliates or the states in which they operate to administer those benefits and to provide services related to those benefits to Class members, which included storing the personal data of Class members on its computers and computer systems. The fees received by Defendant for these services are accrued and paid as a

result of Class members' participation in and payment for these health and pharmaceutical plans.

**B. The Data Breach.**

22. A ransomware attack deploys a type of malicious software that blocks access to a computer system or data, usually by encrypting it, until the victim pays a fee to the attacker.[2]

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

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

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

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

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

/ / /

/ / /

/ /

[2] https://www.proofpoint.com/us/threat-reference/ransomware.

**Notice of Data Incident**

*What Happened*

On April 11, 2020, Magellan Health discovered it was targeted by a ransomware attack. The unauthorized actor gained access to Magellan Health's systems after sending a phishing email on April 6 that impersonated a Magellan Health client. Once the incident was discovered, Magellan Health immediately retained a leading cybersecurity forensics firm, mediation 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 Health corporate server, which included some of your personal information. In limited instances, and only with respect to certain current employers, the unauthorized actor also used a piece of malware designed to steal login credentials and passwords. At this point, we ae not aware of any fraud or misuse 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 names, address, employee ID number, and W-2 OR 1099 details such as Social Security number of Taxpayer ID number and, in limited circumstances, may also include usernames and passwords

*What We Are Doing*

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.[3]

Upon information and belief, this notice was sent to 50410 persons, and was reported to the US Department of Health and Human Services on June 12, 2020.

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

[3] https://oag.ca.gov/system/files/Magellan%20-%20Sample%20Individual%20Notice.pdf

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

***Notice of Security Incident***

> Magellan Health, Inc. and its subsidiaries and affiliates ("Magellan") recently discovered a ransomware attack. We are providing notice of this incident, along with background information of the incident and steps that those affected can take.
>
> *What Happened*
>
> On April 11, 2020 we discovered that we were the target of a ransomware attack. Immediately after discovering the incident we retained a leading cybersecurity forensics firm, Mandiant, to help conduct a thorough investigation of the incident. The investigation revealed that the incident may have affected personal information.
>
> **We have no evidence that any personal data has been misused.**
>
> *What Information Was Involved*
>
> The personal information included names and one or more of the following: treatment information, health insurance account information, member ID, other health-related information, email addresses, phone numbers, and physical addresses. In certain instances, Social Security numbers were also affected.
>
> *What Are We Doing*
> We immediately reported the incident to, and are working closely with, law 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.

A copy of this second notice is posted on Defendant's website.[4]

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

[4] https://www.magellanhealth.com/news/security-incident/

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

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

33. On June 26, 2020, Defendant issued a notice of the Data Breach to persons enrolled in health plans serviced by Defendant.

34. The June 26, 2020 notice of data breach states, in pertinent part:

> Magellan Health, Inc. ("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.
>
> *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 the incident may have affected your personal information. At this point, we are not aware of any fraud or misuse of any of your personal information as a result of the incident, but are notifying you out of an abundance of caution.
>
> *What Information Was Involved*
>
> The personal information accessed by the unauthorized actor included your Social Security number and/or other financial information and possibly included names and one or more of the following: treatment information, health insurance account information, member ID, other health-related information, email addresses, phone numbers, and physical addresses. In certain instances, Social Security numbers were also affected.

*What Are We 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 have implemented additional security protocols designed to protect our network, email environment, systems, and personal information.

35. While clearly related to the same ransomware attack and Data Breach as the May 15, 2020 Notice, the June 26, 2020 notice varies markedly from the May notice, in that the June 26, 2020, reveals that the exfiltrated data included Plaintiff Leather's Social Security number.

36. This is the second cyberattack in less than a year that Defendant Magellan allowed to happen through inadequate email handling procedures and other data security deficiencies. On May 28, 2019, an unauthorized third party gained access to a Magellan employee email account through a commonplace phishing attack that resulted in the exposure of sensitive patient PHI and PII. Magellan gave notice of this prior data breach on or about November 8, 2019. Magellan is already the subject of another lawsuit pending in the United States District Court for the District of Arizona, Phoenix Division, styled Deering v. Magellan Health, Inc. et al., Case 2:20-cv-00747-SPL (D. Ariz., filed Apr. 17, 2020), arising out of that prior data breach.[5]

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

37. Magellan Health has established a Privacy Policy wherein it details the PII it collects from employees and its standards to maintain the security and integrity of such data.[6]

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

---

[5] This action and the prior lawsuit are not related, as they arise from two separate incidents.

[6] 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).

**D. Magellan Health's Patient Privacy Policies.**

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

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

> HIPAA outlines strict guidelines to ensure the privacy and confidentiality of your Personal Health Information (PHI) such as your name or medical information. These guidelines require that your PHI be used for purposes of treatment, payment and health plan operations, and not for purposes unrelated to health care.[7]

41. Defendant assures consumers that "[y]our personal privacy is important to us."[8] Magellan Health's Privacy Policy further states: "Magellan uses physical, technical, and administrative safeguards to protect any personally identifiable data stored on its computers. Only authorized employees and third parties have access to the information you provide to Magellan for providing service to you."[9]

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

42. Data breaches have become widespread. In 2016, the number of U.S. data breaches surpassed 1,000, a record high and a forty percent increase in the number of data breaches from the previous year. In 2017, a new record high of 1,579 breaches were

---

[7] https://www.magellancompletecareoffl.com/utility/privacy-policy/ (last visited 6/28/2020)

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

[9] *Id.*

reported, representing a 44.7 percent increase over 2016. In 2018, there was an extreme jump of 126 percent in the number of consumer records exposed from data breaches. In 2019, there was a 17 percent increase in the number of breaches (1,473) over 2018, with 164,683,455 sensitive records exposed.[10]

43. What's more, companies in the business of storing and maintaining PII, such as Magellan Health are among the most targeted—and therefore at risk— for cyber-attacks.[11]

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

44. The healthcare industry is even more at known risk of cyber-attack. The number of data breaches in the healthcare sector skyrocketed in 2019, with 525 reported breaches exposing nearly 40 million sensitive records (39,378,157), compared to only 369 breaches that exposed just over 10 million sensitive records (10,632,600) in 2018.[12]

45. Phishing cyberattacks against healthcare organizations are targeted. According to the 2019 Health Information Management Systems Society, Inc. ("HIMMS") Cybersecurity Survey, "[a] pattern of cybersecurity threats and experiences is discernable across US healthcare organizations. Significant security incidents are a near-universal experience in US healthcare organizations with many of the incidents initiated by bad actors, leveraging e-mail as a means to compromise the integrity of their targets."[13] "Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From Social Security and insurance policies to next of kin and credit cards, no other

---

[10] https://www.idtheftcenter.org/identity-theft-resource-centers-annual-end-of-year-data-breach-report-reveals-17-percent-increase-in-breaches-over-2018/

[11] https://www.cshub.com/attacks/articles/top-8-industries-reporting-data-breaches-in-the-first-half-of-2019

[12] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf

[13] https://www.himss.org/himss-cybersecurity-survey (last accessed June 20, 2020)

organization, including credit bureaus, have so much monetizable information stored in their data centers."[14]

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

> Medical identity theft is costly to consumers. Unlike credit-card fraud, victims of medical identity theft can suffer significant financial consequences. Sixty-five percent of medical identity theft victims had to pay an average of $13,500 to resolve the crime. In some cases, they paid the health care provider, repaid the insurer for services obtained by the thief, or they engaged an identity-service provider or legal counsel to help resolve the incident and prevent fraud.
>
> Those who have resolved the crime spent, on average, more than 200 hours on such activities as working with their insurer or health-care provider.
>
> Medical identity theft can have a negative impact on reputation. Forty-five percent of respondents said medical identity theft affected their reputation mainly because of embarrassment due to disclosure of sensitive personal health conditions; 19 percent of respondents believed the theft caused them to miss out on career opportunities. Three percent said it resulted in the loss employment.[15]

**G. Defendant Acquires, Collects, and Stores Plaintiffs' and Class Members' PII and PHI.**

47. As its Privacy Policy makes clear, Magellan Health acquires, collects, and stores a massive amount of personally identifiable information ("PII") on its employees, former employees and beneficiaries.

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

---

[14] https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last accessed June 20, 2020)

[15] 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)

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

50. By obtaining, collecting, creating, and using Plaintiffs' and Class Members' PII and PHI, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PII and PHI from disclosure.

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

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

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

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

54. Personally identifiable information is a valuable commodity to identity thieves. As the FTC recognizes, with PII identity thieves can commit an array of crimes including identify theft, medical and financial fraud.[16] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII on multiple underground Internet websites.

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

---

[16] Federal Trade Commission, *Warning Signs of Identity Theft,* https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft

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

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

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

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

59. It was therefore foreseeable that the failure to adequately safeguard Plaintiffs and Class Members' Private Information would result in one or more types of

injuries to Plaintiffs and Class Members.

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

60. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[17]

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

62. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[19]

63. The FTC has brought enforcement actions against businesses for failing to

---

[17] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[18] https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business

[19] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

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

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

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

66. Companies in the business of storing and maintaining PII and PHI, such as Magellan Health, have been identified as being particularly vulnerable to cyber-attacks because of the value of the PII and PHI which they maintain. Cybersecurity firms have promulgated a series of best practices that a minimum should be implemented by sector participants including, but not limited to: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.[20]

67. The Data Breach appears to have been caused by "a standard credential phishing attack or due to credential reuse on another site."[21]

---

[20] https://insights.datamark.net/addressing-bpo-information-security/

[21] https://www.scmagazine.com/home/security-news/phishing/canon-breach-exposes-personal-data-of-current-former-ge-employees-beneficiaries/.

68. Cybersecurity experts have explicitly noted that phishing attacks can be prevented with adequate staff security training.[22]

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

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

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

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

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

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

74. As a direct and proximate result of Defendant' wrongful actions and inactions, Plaintiffs and Class Members have been placed at an imminent, immediate,

[22] https://www.passportalmsp.com/blog/security-awareness-training-can-protect-against-phishing-attacks.

and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[23]

75. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GOA Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[24]

76. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[25]

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

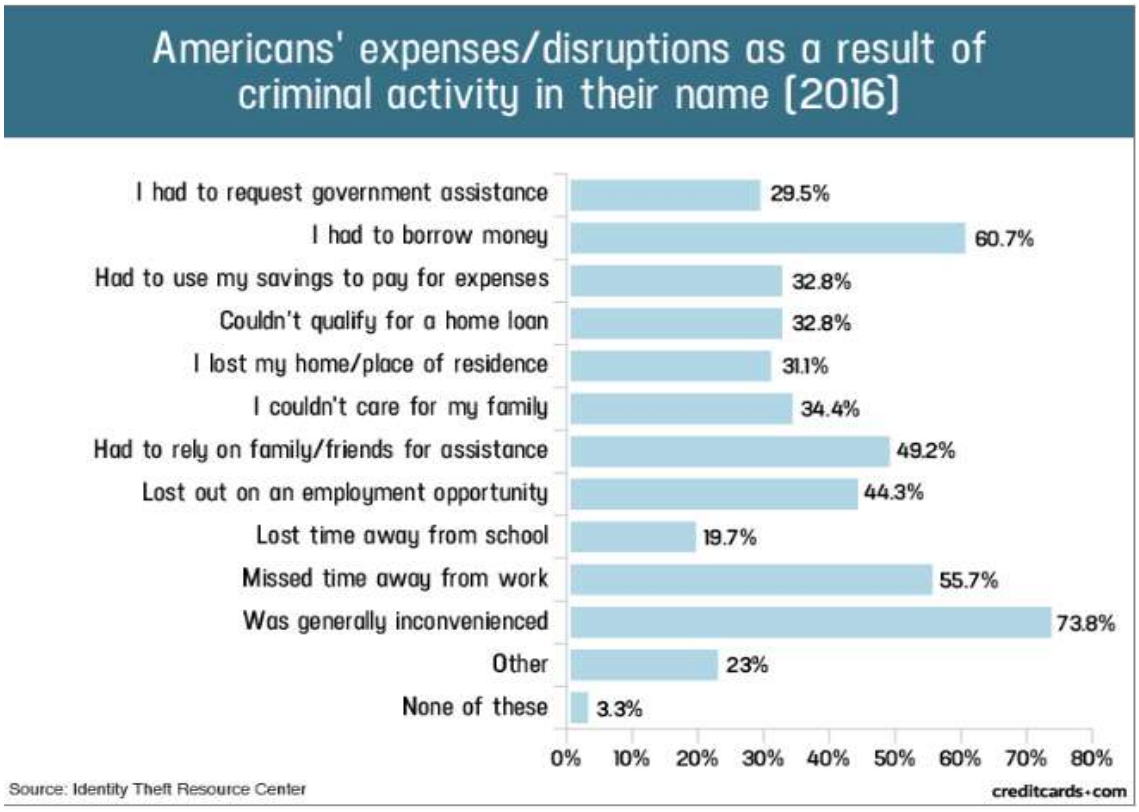
---

[23] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013 available at https://www.bjs.gov/content/pub/pdf/vit12.pdf

[24] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Apr. 12, 2019) ("GAO Report").

[25] *See* https://www.identitytheft.gov/Steps (last visited April 12, 2019).

78. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[26]




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

79. What's more, PII constitutes a valuable property right, the theft of which is gravely serious.[27] 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.

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

*See* GAO Report, at p. 29.

81. PII and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

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

---

[27] *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).

**L. Plaintiffs' and Class Members' Damages**.

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

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

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

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

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

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

89. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax

return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

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

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

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

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

94. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;
b. Canceling and reissuing credit and debit cards;
c. Purchasing credit monitoring and identity theft prevention;
d. Addressing their inability to withdraw funds linked to compromised accounts;
e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;
f. Placing “freezes” and “alerts” with credit reporting agencies;
g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

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

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

97. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

## V. CLASS ACTION ALLEGATIONS

98. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated ("the Class").

99. Plaintiffs propose the following Class definitions, subject to amendment as appropriate:

The Nationwide Class: All persons whose PII and PHI was compromised as a result of the Ransomware Attack that Magellan Health discovered on or about April 11, 2020.

The Missouri Class: All persons residing in Missouri whose PII and PHI was compromised as a result of the Ransomware Attack that Magellan Health discovered on or about April 11, 2020.

The Tennessee Class: All persons residing in Tennessee whose PII and PHI was compromised as a result of the Ransomware Attack that Magellan Health discovered on or about April 11, 2020.

The Pennsylvania Class: All persons residing in Pennsylvania whose PII and PHI was compromised as a result of the Ransomware Attack that Magellan Health discovered on or about April 11, 2020.

The New York Class: All persons residing in New York whose PII and PHI was compromised as a result of the Ransomware Attack that Magellan Health discovered on or about April 11, 2020.

The Employee Class: All current and former employees of Magellan whose PII and PHI was compromised as a result of the Ransomware Attack that Magellan Health discovered on or about April 11, 2020.

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

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

102. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Class consists of approximately 365,000 employees, former employees, beneficiaries, and patients of Defendant Magellan Health and its affiliates named herein whose data was compromised in the Data Breach.

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

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' PII and PHI;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their PII and PHI;

f. Whether Defendant breached its duty to Class Members to safeguard their PII and PHI;

g. Whether computer hackers obtained Class Members' PII and PHI in the Data Breach;

h. Whether Defendant knew or should have known that their data security systems and monitoring processes were deficient;

i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant' misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant' s conduct was per se negligent;

l. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

m. Whether Defendant was unjustly enriched;

n. Whether Defendant failed to provide notice of the Data Breach in a timely manner, and;

o. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

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

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

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

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

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

109. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

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

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

/ / /

/ / /

/ / /

/ / /

/ /

## VI. CAUSES OF ACTION

### COUNT I
### NEGLIGENCE
### (On Behalf of Plaintiff and the Nationwide Class, Or, Alternatively, Plaintiff Griffey and the Missouri Class, Plaintiff Rayam and the Tennessee Class, Plaintiff Domingo and the Pennsylvania Class, and Plaintiff Leather and the New York Class)

111. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 111 above as if fully set forth herein.

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

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

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

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

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

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

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

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

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

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII and PHI;
b. Failing to adequately monitor the security of their networks and systems;
c. Failing to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;
d. Allowing unauthorized access to Class Members' PII and PHI;
e. Failing to detect in a timely manner that Class Members' PII and PHI had been compromised; and

f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

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

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

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

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

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

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

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

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

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

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

**COUNT II**
**NEGLIGENCE *PER SE***
**(On Behalf of Plaintiff and the Nationwide Class, Or, Alternatively, Plaintiff Griffey and the Missouri Class, Plaintiff Rayam and the Tennessee Class, Plaintiff Domingo and the Pennsylvania Class, and Plaintiff Leather and the New York Class)**

131. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 111 above as if fully set forth herein.

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

133. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant's, of failing to use reasonable measures to protect PII and PHI. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

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

135. Defendant's violation of Section 5 of the FTC Act constitutes negligence per se as Defendant's violation of the FTC Act establishes the duty and breach elements of negligence.

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

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

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

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

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

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

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

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

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

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

**COUNT III**
**BREACH OF IMPLIED CONTRACT**
**(On Behalf of Plaintiffs Griffey, Rayam, Domingo and the Employee Class)**

146. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 111 above as if fully set forth herein.

147. 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.

148. 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.

149. 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.

150. 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.

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

152. 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.

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

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

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

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

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

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

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

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

161. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

**COUNT IV**
**VIOLATION OF THE NEW YORK**
**GENERAL BUSINESS LAW § 349**
**(On Behalf of Plaintiff Leather and the New York Class)**

162. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 111 above as if fully set forth herein.

163. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a), including but not limited to the following:

164. Defendant misrepresented material facts to Plaintiff and the Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Class members' PHI and PII from unauthorized disclosure, release, data breaches, and theft;

165. Defendant misrepresented material facts to Plaintiff and the Class by representing that they did and would comply with the requirements of federal and state laws pertaining to the privacy and security of Class members' PHI and PII;

166. Defendant omitted, suppressed and concealed material facts of the inadequacy of its privacy and security protections for Class members' PHI and PII;

167. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Class members' PHI and PII, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45);

168. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the data breach to the Class in a timely and accurate manner, contrary to the duties imposed by N.Y. Gen. Bus. Law § 899-aa(2). At all times relevant herein, Leather and members of the New York Class were residents of the State of New York and were deceived in New York by the misconduct alleged herein.

169. Defendant knew or should have known that the its computer systems and data security practices were inadequate to safeguard the Class members' PHI and PII entrusted to it, and that risk of a data breach or theft was highly likely.

170. Defendant should have disclosed this information because Defendant was in a superior position to know the true facts related to the defective data security.

171. Defendant's failure constitutes false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiff and Class members) regarding the security of Magellan Health's network and aggregation of PHI and PII.

172. The representations upon which consumers (including Plaintiff and Class members) relied were material representations (e.g., as to Defendant's adequate protection of PHI and PII), and consumers (including Plaintiff and Class members) relied on those representations to their detriment.

173. Defendant's conduct is unconscionable, deceptive, and unfair, as it is likely to, and did, mislead consumers acting reasonably under the circumstances. As a direct and proximate result of Defendant's conduct, Plaintiff and other Class members have been harmed, in that they were not timely notified of the data breach, which resulted in profound vulnerability to their personal information and other financial accounts.

174. As a direct and proximate result of Defendant's unconscionable, unfair, and deceptive acts and omissions, Plaintiff's and Class members' PHI and PII was disclosed to third parties without authorization, causing and will continue to cause Plaintiff and Class members damages, as well as to the public interest and consumers at large in New York.

175. Plaintiff and Class members seek relief under N.Y. Gen. Bus. Law § 349(h), including, but not limited to, actual damages, treble damages, statutory damages, injunctive relief, and/or attorney's fees and costs.

**COUNT V**
**UNJUST ENRICHMENT**
**(On Behalf of Plaintiffs and All Class Members)**

176. Plaintiffs restate and reallege paragraphs 1 through 111 above as if fully set forth herein.

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

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

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

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

181. Plaintiffs and Class Members have no adequate remedy at law.

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

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

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

/ / /

/ / /

/ /

**COUNT VI**
**ARIZONA CONSUMER FRAUD ACT ("ACFA")**
**Ariz. Rev. Stat. §§ 44-1521, et seq.**
**(On Behalf of Plaintiffs and the Nationwide Class, Or, Alternatively, Plaintiff Griffey and the Missouri Class, Plaintiff Rayam and the Tennessee Class, Plaintiff Domingo and the Pennsylvania Class, and Plaintiff Leather and the New York Class)**

185. Plaintiffs restate and reallege paragraphs 1 through 111 as if fully set forth herein.

186. The ACFA provides in pertinent part: "The act, use or employment by any person of any deception, deceptive or unfair act or practice, fraud, false pretense, false promise, misrepresentation, or concealment, suppression or omission of any material fact with intent that others rely on such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise whether or not any person has in face been misled, deceived or damaged thereby, is declared to be an unlawful practice." Ariz. Rev. Stat. § 44-1522.

187. Plaintiffs and Class Members are "persons" as defined by Ariz. Rev. Stat. § 44-1521(6).

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

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

a. Failing to maintain sufficient security to keep Plaintiffs' and Class Members' confidential medical, financial and personal data from being hacked and stolen;

b. Failing to disclose the Data Breach to Class Members in a timely and accurate manner, in violation of Ariz. Rev. Stat. § 18-552(B);

c. Misrepresenting material facts, pertaining to the sale of health benefit services by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Class Members' PHI and PII from unauthorized disclosure, release, data breaches, and theft;

d. Misrepresenting material facts, in connection with the sale of health benefit services by representing that they did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Class Members' PHI and PII;

e. Omitting, suppressing, and concealing the material fact of the inadequacy of the data privacy and security protections for Class Members' PHI and PII;

f. Engaging in unfair, unlawful, and deceptive acts and practices with respect to the sale of health benefit services by failing to maintain the privacy and security of Class Members' PHI and PII, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws, including HIPAA and Section 5 of the FTC Act;

g. Engaging in unlawful, unfair, and deceptive acts and practices with respect to the sale of health benefit services by failing to disclose the Data Breach to Class Members in a timely and accurate manner;

h. Engaging in unlawful, unfair, and deceptive acts and practices with respect to the sale of health benefit services by failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Class Members' PHI and PII from further unauthorized disclosure, release, data breaches, and theft.

190. The above unlawful, unfair, and deceptive acts and practices by Magellan were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial

injury to Plaintiffs and Class Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

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

192. As a direct and proximate result of Defendant's deceptive acts and practices, the Class Members suffered an ascertainable loss of money or property, real or personal, as described above, including the loss of their legally protected interest in the confidentiality and privacy of their PHI and PII.

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

**PRAYER FOR RELIEF**

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

A. For an Order certifying this action as a Class action and appointing Plaintiffs and their counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

D. For equitable relief requiring restitution and disgorgement of the revenues

wrongfully retained as a result of Defendant's wrongful conduct;

E. Ordering Defendant to pay for not less than seven years of credit monitoring services for Plaintiffs and the Class;

F. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

G. For an award of punitive damages, as allowable by law;

H. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

I. Pre- and post-judgment interest on any amounts awarded; and

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: July 22, 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

**DEYOUNG & ASSOCIATES**
Neal A. DeYoung (*Pro Hac Vice* to be filed)
One Reservoir Office Park
Southbury, Ct. 06488
Telephone: (203) 731-7558
Email: neal@deyounglegal.com

*Attorneys for Plaintiffs*