

1 Elaine A. Ryan (AZ Bar #012870)
2 Carrie A. Laliberte (AZ Bar #032556)
3 BONNETT, FAIRBOURN, FRIEDMAN
& BALINT, P.C.
4 2325 E. Camelback Rd., Suite 300
5 Phoenix AZ 85016
6 Telephone: (602) 274-1100
7 Email: erylal@bffb.com
8 claliberte@bffb.com

6 Patricia N. Syverson (AZ Bar #020191)
7 BONNETT, FAIRBOURN, FRIEDMAN
& BALINT, P.C.
8 600 W. Broadway, Suite 900
9 San Diego, California 92101
10 Telephone: (619) 798-4593
11 Email: psyverson@bffb.com

10 *As local counsel on behalf of:*

11 John A. Yanchunis (*To Be Admitted Pro Hac Vice*)
12 Patrick A. Barthle (*To Be Admitted Pro Hac Vice*)
13 MORGAN & MORGAN
14 COMPLEX LITIGATION GROUP
15 201 N. Franklin Street, 7th Floor
16 Tampa, Florida 33602
17 Telephone: (813) 223-5505
18 Email: jyanchunis@forthepeople.com
19 pbarthle@forthepeople.com

16 Counsel for Plaintiff and the Putative Class
[Additional Counsel on Signature Page]

17 **UNITED STATES DISTRICT COURT**
18 **DISTRICT OF ARIZONA**
19 **PHOENIX DIVISION**

20 CAROL DEARING, on behalf of herself
and all others similarly situated,

21 Plaintiff,

22 v.

23 MAGELLAN HEALTH INC. AND
24 MAGELLAN RX MANAGEMENT,
LLC,

25 Defendants.
26

Case No.:

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

27
28

1 Plaintiff Carol Dearing, by and through her undersigned counsel, brings this class
2 action lawsuit against Magellan Health Inc. (“Magellan Health”) and Magellan Rx
3 Management, LLC (“Magellan Rx”) (and together, “Magellan” or “Defendants”), on behalf
4 of herself and all others similarly situated, and alleges, based upon information and belief
5 and the investigation of her counsel as follows:

6 **INTRODUCTION**

7 1. Magellan is a large healthcare service provider that, among other things,
8 directly manages pharmaceutical benefits for their members’ patients, including those
9 participating in state-sponsored Medicaid programs such as TennCare of Tennessee of
10 which Plaintiff is a member.¹

11 2. As part of its contractual relationship with TennCare and several other
12 providers, Magellan administers the pharmaceutical benefits under the state-sponsored
13 Medicaid plan throughout the applicable state. As a result of Plaintiff’s participation in
14 TennCare, Magellan received fees from TennCare and/or the state of Tennessee to
15 administer those benefits and to provide services related to those benefits to Plaintiff and
16 other TennCare beneficiaries, which included storing the personal data of Plaintiff and
17 others on their computers and computer systems.

18 3. On or about November 8, 2019, Magellan notified affected patients that an
19 employee, who manages member data for various health plans, fell for a phishing scheme
20 that compromised his/her email and resulted in exposure of the personally identifiable
21 information (“PII”) and protected health information (“PHI”) (collectively, “PII”) of tens of
22 thousands of individuals, including Plaintiff and 44,000 other TennCare participants (the
23

24
25 ¹ TennCare is the State of Tennessee’s Medicaid program that provides health care for
26 approximately 1.4 million Tennesseans consisting primarily of low-income pregnant
27 women, children, and individuals who are elderly or have a disability. TennCare covers
28 approximately 20 percent of the state’s population, 50 percent of the state’s births, and 50
percent of the state’s children. <https://www.tn.gov/tenncare/information-statistics/tenncare-overview.html> (last visited April 13, 2020).

1 “Data Breach”). The exposed PHI and PII included names, Social Security Numbers,
2 member IDs, health plans, provider names, and the names of the drugs that members have
3 been prescribed.

4 4. On July 5, 2019, Magellan discovered the Data Breach, which occurred on
5 May 28, 2019. A subsequent investigation revealed that at least one other employee’s email
6 account had also been accessed by an unauthorized third party as part of the Data Breach.

7 5. Despite having known about the Data Breach since early July, Magellan
8 inexplicably delayed more than four months before it alerted the affected patients that their
9 PII had been unlawfully exposed.

10 6. The Data Breach was a direct result of Defendants’ failure to implement
11 adequate and reasonable cyber-security procedures and protocols necessary to protect
12 patient PII.

13 7. Defendants disregarded the rights of Plaintiff and Class Members (defined
14 below) by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take
15 adequate and reasonable measures to ensure their data systems were protected against
16 unauthorized intrusions; failing to disclose that they did not have adequately robust
17 computer systems and security practices to safeguard patient PHI and PII; failing to take
18 standard and reasonably available steps to prevent the Data Breach; failing to monitor and
19 timely detect the Data Breach; and failing to provide Plaintiff and Class Members with
20 prompt and accurate notice of the Data Breach.

21 8. As a result of Defendants’ failure to implement and follow basic security
22 procedures, patient PHI and PII is now in the hands of thieves. Plaintiff and Class Members
23 have had to spend, and will continue to spend, significant amounts of time and money in an
24 effort to protect themselves from the adverse ramifications of the Data Breach and will
25 forever be at a heightened risk of identity theft and fraud.

26 9. Plaintiff, on behalf of all others similarly situated, alleges claims for
27 negligence, negligence per se, breach of implied contract, unjust enrichment, , and
28

1 violations of the Arizona Consumer Fraud Act, and seeks injunctive and declaratory relief
2 to, *inter alia*, compel Defendants to adopt reasonably sufficient security practices to
3 safeguard patient PHI and PII that remains in their custody in order to prevent incidents
4 like the Data Breach from reoccurring in the future.

5 **PARTIES**

6 10. Plaintiff Carol Dearing, a resident of Sparta, Tennessee, is a TennCare
7 participant and obtained her prescriptions through Magellan Rx. On or about November 8,
8 2019, Ms. Dearing was sent a notice from Magellan Rx of a Data Breach that involved her
9 highly sensitive PHI and PII, including her name, Social Security Number, health plan ID
10 number, health plan name, provider name, and drug names (the “Notice”).²

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

14 12. Defendant Magellan Rx is a division of Magellan Health that provides,
15 among other things, clinical and financial management of pharmaceuticals paid under
16 medical and pharmacy benefit programs. Specifically, Magellan Rx offers pharmacy benefit
17 management services, pharmacy benefit administration for state Medicaid and other
18 government sponsored programs; pharmaceutical dispensing operations; clinical and
19 formulary management programs; medical pharmacy management programs; and programs
20 for the management of specialty drugs that treat complex conditions. The company provides
21 services to health plans and other managed care organizations, employers, labor unions,
22 various military and governmental agencies, and third-party administrators.

23 13. According to filings with the Arizona Corporation Commission, Magellan
24 Rx is incorporated in the state of Delaware. Its CEO, however, Mostafa Kamal is located
25 _____

26 ² A true and copy of the Notice is attached hereto as Exhibit A. The Notice appears to have
27 been sent from ID Experts, a third party identity theft and protection service company, of
28 Everett, Washington on behalf of Magellan Rx and was signed by John J. DiBernardi, Jr.,
the Senior Vice President and Chief Compliance Officer for Magellan Health.

1 at the company's corporate office in Scottsdale, Arizona where Magellan Rx maintains its
2 principal place of business.

3 14. Magellan Rx operates through a website portal, where it interacts directly
4 with members of the programs it offers.³ It provides patients such as Plaintiff and Class
5 Members with pharmacy benefit cards that they must use to obtain medications. Moreover,
6 patients are provided telephone numbers that are answered by Magellan and are to be used
7 in the event they have questions or issues with their prescriptions.

8 JURISDICTION AND VENUE

9 15. This Court has subject matter jurisdiction over this action under the Class
10 Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million,
11 exclusive of interest and costs. There are at least 44,000 putative Class Members, most of
12 whom have different citizenship from Magellan.

13 16. This Court has jurisdiction over Defendants, which operate and are
14 headquartered in this District. The computer systems implicated in this Data Breach are
15 likely based in this District. Through their business operations in this District, Magellan
16 intentionally avails themselves of the markets within this District to render the exercise of
17 jurisdiction by this Court just and proper.

18 17. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a
19 substantial part of the events and omissions giving rise to this action occurred in this District.
20 Defendants are based in this District, maintain patient PHI and PII in the District, and have
21 caused harm to Plaintiff and Class Members through their actions in this District.

22 STATEMENT OF FACTS

23 *A. The Data Breach*

24 18. On July 5, 2019, Magellan learned that an unauthorized third party gained
25 access to an employee email account through a commonplace phishing attack which
26

27 _____
28 ³ <https://www1.magellanrx.com/> (last visited April 13, 2020).

1 occurred on May 28, 2019 and resulted in the exposure of sensitive patient PHI and PII.
2 The exposed sensitive PHI and PII included patient: names, Social Security Numbers, health
3 plan member ID numbers, health plan names, provider information, and prescription drug
4 names.

5 19. Despite the Data Breach occurring on May 28, 2019, Magellan did not learn
6 of the breach until July 5, 2019 – over a month later. Magellan did not have sufficient
7 security measures in place to promptly detect much less prevent the Breach.

8 20. And, despite having become aware of the Data Breach in July 2019,
9 Magellan waited more than 4 months to notify affected patients.

10 21. The notice sent by Magellan to Plaintiff and Class Members stated, in
11 relevant part:

12
13 November 8, 2019

14 Re: Notice of Possible Data Breach

15 Magellan Rx Management, a subsidiary of Magellan Health, Inc. (“Magellan”),
16 manages the pharmacy benefits for TennCare and its members. We review health
17 care services to make sure they are medically necessary and should be paid.

18 This letter is to let you know that some information about you may have been put
19 at risk.

20 **What Happened**

21 On July 5, 2019, Magellan learned that one of our employee’s email accounts had
22 been hacked by an unknown third-party (“hacker”) on May 28, 2019. Our
23 information security team immediately took steps to lockdown this employee’s
24 account and make sure no others could access it. We also immediately undertook
25 an investigation to find out if any other email accounts were hacked. We believe
26 that the hacker was trying to access our employee’s email account to send out
27 spam. Spam is unwanted email from unknown people. We also believe he or she
28 had no plan to view, read or do anything with the emails. We cannot say for sure
that no emails were seen. While we have no proof that the hacker saw any emails,
we are being extra careful. We want you to know that your information was in at
least one email.

What Information Was Involved

1
2 We understand you may be worried about this. The emails that may have been
3 seen had information such as:

- 4 • Your name
- 5 • Your Social Security number
- 6 • Your health plan member ID number
- 7 • The name of your health plan
- 8 • Your provider
- 9 • Drug name

10 **What You Can Do**

11 While we do not know of any attempt by the hacker to access or use your personal
12 information, we are offering you services through ID Experts®, the data breach
13 and recovery services expert, to provide you with MyIDcare™. MyIDCare
14 services include: 12 months of Credit and CyberScan monitoring, a \$1,000,000
15 insurance reimbursement policy, and fully managed ID theft recovery services.
16 With this protection, MyIDCare will help you resolve issues if your identity is
17 compromised.⁴

18 22. While 44,000 TennCare patients were among the first to get notice, Magellan
19 subsequently revealed that the Data Breach extended to patients of other providers across
20 the United States as well:

21 **Important Health Plan Announcement**

22 **Important announcement for Health Plan members receiving pharmacy
23 services managed by Magellan Rx Management:**

24 On July 5, 2019 Magellan Health's subsidiary, Magellan Rx Management,
25 discovered a potential data breach related to protected health information of the
26 following health plans:

- 27 • Posted on 11/13/19 – Florida Blue
- 28 • Posted on 11/18/19 – Independent Health
- Posted on 11/22/19 – Emblem
- Posted on 11/27/19 – Alliant Health Plans

⁴ See Exhibit A.

- 1 • Posted on 11/27/19 – ConnectiCare Inc
- 2 • Posted on 11/27/19 – Horizon BCBS NJ

3 We found that an anonymous, unauthorized third party accessed the email
4 accounts of an employee who handles member data for various health plans. The
5 unauthorized access occurred on May 28, 2019. We immediately secured the
6 employee’s email account and conducted a thorough investigation of all
7 employee email accounts and all other Magellan systems. We believe that the
8 impacted employee may have been the target of a phishing scam and that the
9 purpose of the unauthorized access to the email account was to send out email
10 spam.

11 As a result of the hacking incident, member protected health information may
12 potentially have been accessed. The affected email account contained protected
13 health information that included health benefits information, which may have
14 included member name, date of birth, member address, member ID, provider
15 name, authorization determination and/or number, claim number, date(s) of
16 service, drug name, billing codes, or benefit descriptions such as diagnosis or
17 procedure. The employee’s email account also included the Social Security
18 Numbers (SSN) of members of some health plans.⁵

13 ***B. Magellan’s Privacy Policies***

14 23. As healthcare service providers, Defendants are bound by the Health
15 Insurance Portability and Accountability Act of 1996 (“HIPAA”), which requires subject
16 providers to comply with a series of administrative, physical security, and technical security
17 requirements in order to protect patient information. Among other things, it mandates
18 medical providers develop, publish, and adhere to a privacy practice.

19 24. Magellan recognizes their obligations under HIPAA along with the
20 commensurate obligation to safeguard and protect patient PHI and PII, assuring users that
21 “[y]our personal privacy is important to us.”⁶ Magellan Health’s Privacy Policy further
22 states:

23 **Security**

24 A range of security features protect the privacy of any individualized information
25 you provide over a secure sign-in to the Magellan website. During transmission
26

27 ⁵ <https://www1.magellanrx.com/home/2516-2/> (last visited April 13, 2020).

28 ⁶ <https://www1.magellanrx.com/privacy-policy/> (last visited April 13, 2020).

1 over a secure sign-in website, your privacy is protected by 128-bit or greater
2 cryptographic security. Other security safeguards are also in place.

3 Magellan uses physical, technical, and administrative safeguards to protect any
4 personally identifiable data stored on its computers. Only authorized employees
5 and third parties have access to the information you provide to Magellan for
6 providing service to you.

7 **HIPAA**

8 HIPAA is the federal Health Insurance Portability and Accountability Act of 1996
9 (“HIPAA”).

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

14 ***C. Prevalence of Cyber Attacks and Susceptibility of the Healthcare Sector***

15 25. Cyber-attacks come in many forms. Phishing attacks are among the oldest,
16 most common, and well known. In simple terms, phishing is a method of obtaining personal
17 information using deceptive e-mails and websites. The goal is to trick an e-mail recipient
18 into believing that the message is something they want or need from a legitimate or
19 trustworthy source and to subsequently take an action such as clicking on a link or
20 downloading an attachment. The fake link will typically mimic a familiar website and
21 require the input of credentials. Once input, the credentials are then used to gain
22 unauthorized access into a system. “It’s one of the oldest types of cyber-attacks, dating
23 back to the 1990s” and one that every organization with an internet presence is aware.”⁸ It
24 remains the “simplest kind of cyberattack and, at the same time, the most dangerous and
25 effective.”⁹

26 ⁷ See, e.g., <https://www.magellanhealth.com/privacy-policy/> (last visited April 13, 2020).

27 ⁸ What is phishing? How this cyber attack works and how to prevent it, CSO Online,
28 February 20, 2020, [https://www.csoonline.com/article/2117843/what-is-phishing-how-
this-cyber-attack-works-and-how-to-prevent-it.html](https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html) (last visited April 13, 2020).

⁹ *Phishing*, Malwarebytes, <https://www.malwarebytes.com/phishing/> (last visited April 13,
2020).

1 26. Phishing attacks are well known and understood by the cyber-protection
2 community and are generally preventable with the implementation of a variety of proactive
3 measures such as sandboxing inbound e-mail¹⁰, inspecting and analyzing web traffic,
4 penetration testing¹¹, and employee education, among others.

5 27. In 2016, the number of U.S. data breaches surpassed 1,000, a record high
6 and a 40% increase in the number of data breaches from the previous year.¹² In 2017, a new
7 record high of 1,579 breaches were reported, representing a 44.7% increase over 2016.¹³

8 28. In 2018, the healthcare sector reported the second largest number of breaches
9 among all measured sectors and the highest rate of exposure per breach.¹⁴ Indeed, healthcare
10 related data is among the most sensitive and personally consequential when compromised.
11 A report focusing on healthcare breaches found that the “average total cost to resolve an
12 identity theft-related incident...came to about \$20,000,” and that the victims were often
13 forced to pay out-of-pocket costs for health care they did not receive in order to restore
14

15
16 ¹⁰ Sandboxing is an automated process whereby e-mail with attachments and links are
17 segregated to an isolated test environment, or a “sandbox,” wherein a suspicious file or URL
18 may be executed safely.

19 ¹¹ Penetration testing is the practice of testing a computer system, network, or web
20 application to find security vulnerabilities that an attacker could exploit. The main objective
21 of penetration testing is to identify security weaknesses. Penetration testing can also be used
22 to test an organization's security policy, its adherence to compliance requirements, its
23 employees' security awareness and the organization's ability to identify and respond to
24 security incident. The primary goal of a penetration test is to identify weak spots in an
25 organization's security posture, as well as measure the compliance of its security policy, test
26 the staff's awareness of security issues and determine whether -- and how -- the organization
27 would be subject to security disasters. See
28 <https://searchsecurity.techtarget.com/definition/penetration-testing> (last visited April 13,
2020).

¹² Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), available at <https://www.idtheftcenter.org/surveys-studys> (last visited April 13, 2020).

¹³ Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review*, available at <https://www.idtheftcenter.org/2017-data-breaches/> (last visited April 13, 2020).

¹⁴ Identity Theft Resource Center, *2018 End -of-Year Data Breach Report*, available at <https://www.idtheftcenter.org/2018-data-breaches/> (last visited April 13, 2020).

1 coverage.¹⁵ Almost 50% of the victims lost their health care coverage as a result of the
2 incident, while nearly one-third said their insurance premiums went up after the event. Forty
3 percent of the customers were never able to resolve their identity theft at all. Data breaches
4 and identity theft have a crippling effect on individuals and detrimentally impact the
5 economy as a whole.¹⁶

6 29. Healthcare related data breaches have continued to rapidly increase.
7 According to the 2019 HIMSS Cybersecurity Survey, 82% of participating hospital
8 information security leaders reported having a significant security incident in the last 12
9 months, with a majority of these known incidents being caused by “bad actors” such as
10 cybercriminals.¹⁷ “Hospitals have emerged as a primary target because they sit on a gold
11 mine of sensitive personally identifiable information for thousands of patients at any given
12 time. From Social Security and insurance policies to next of kin and credit cards, no other
13 organization, including credit bureaus, have so much monetizable information stored in
14 their data centers.”¹⁸

15 30. Indeed, the HIPAA Journal 2019 Healthcare Data Breach Report
16 demonstrates an upward trend in health sector data breaches over the past 10 years, with
17 2019 reflecting more data breaches than any other year.¹⁹ 2019 represented a 37.4% increase
18
19
20

21 ¹⁵ Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET, March 3, 2010,
22 <https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/> (last visited
23 April 13, 2020).

¹⁶ *Id.*

¹⁷ HIMSS, 2019 HIMSS Cybersecurity Survey, <https://www.himss.org/himss-cybersecurity-survey> (last visited April 13, 2020).

¹⁸ Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, available at <https://www.digitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks> (last visited April 13, 2020).

¹⁹ HIPAA Journal, Healthcare Data Breach Statistics, <https://www.hipaajournal.com/healthcare-data-breach-statistics/> (last visited April 13, 2020).

1 over breaches reported in 2018 with a total number of patient records exposed increasing
2 from 13,947,909 in 2018 to 41,335,889.²⁰

3 31. “Shockingly, the report disclosed that in 2019 alone, the healthcare records
4 of 12.55% of the population of the United States were exposed, impermissibly disclosed, or
5 stolen.”²¹

6 32. As healthcare services providers, Magellan knew, or should have known, the
7 importance of safeguarding patient PHI and PII entrusted to them and of the foreseeable
8 consequences if their data security systems were breached, including the significant costs
9 that would be imposed on their patients as a result of a breach. But Magellan failed to take
10 adequate cyber-security measures to prevent the Data Breach from occurring.

11 ***D. Magellan Acquires, Collects, and Stores Plaintiff’s and Class Members’ PHI and***
12 ***PII***

13 33. Magellan acquires, collects, and stores a massive amount of protected health
14 related information and other personally identifiable data on their members’ patients.

15 34. As a condition of engaging in health services, Magellan requires that these
16 patients entrust them with highly sensitive personal information.

17 35. By obtaining, collecting, using, and deriving a benefit from Plaintiff’s and
18 Class Members’ PHI and PII, Magellan assumed legal and equitable duties and knew or
19 should have known that it was responsible for protecting Plaintiff’s and Class Members’
20 PHI and PII from unauthorized disclosure.

21 36. Plaintiff and Class Members have taken reasonable steps to maintain the
22 confidentiality of their PHI and PII. Plaintiff and Class Members relied on Magellan to keep
23

24
25 ²⁰ *2019 Healthcare Data Breach Report*, HIPAA Journal,
26 <https://www.hipaajournal.com/2019-healthcare-data-breach-report/> (last visited April 13,
2020).

27 ²¹ *Report Reveals Worst State for Healthcare Data Breaches in 2019*, Info Security Group,
28 February 14, 2020, <https://www.infosecurity-magazine.com/news/report-healthcare-data-breaches-in/> (last visited April 13, 2020).

1 their PHI and PII confidential and securely maintained, to use this information for business
2 purposes only, and to make only authorized disclosures of this information.

3 ***E. The Value of Personally Identifiable Information and the Effects of Unauthorized***
4 ***Disclosure***

5 37. Magellan was well-aware that the PHI and PII they collect is highly
6 sensitive, and of significant value to those who would use it for wrongful purposes.

7 38. Personal identifiable information is a valuable commodity to identity thieves.
8 As the FTC recognizes, with identity thieves can commit an array of crimes including
9 identify theft, medical and financial fraud.²² Indeed, a robust “cyber black market” exists in
10 which criminals openly post stolen PII on multiple underground Internet websites.

11 39. While credit card information and associated PII can sell for as little as \$1-
12 \$2 on the black market, protected health information can sell for as much as \$363 according
13 to the Infosec Institute. This is because one’s personal health history (*e.g.*, ailments,
14 diagnosis, surgeries, etc.) cannot be changed.²³ PHI is particularly valuable because
15 criminals can use it to target victims with frauds and scams that take advantage of the
16 victim’s medical conditions or victim settlements. It can be used to create fake insurance
17 claims, allowing for the purchase and resale of medical equipment, or gain access to
18 prescriptions for illegal use or resale.

19 40. The ramifications of Magellan’s failure to keep their patients’ PII secure are
20 long lasting and severe. Once PHI and PII is stolen, fraudulent use of that information and
21 damage to victims may continue for years.

22 41. For example, the Social Security Administration has warned that identity
23 thieves can use an individual’s Social Security Number to apply for additional credit lines.

24
25 ²² Federal Trade Commission, *Warning Signs of Identity Theft*,
26 <https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft> (last visited April
13, 2020).

27 ²³ Center for Internet Security, *Data Breaches: In the Healthcare Sector*,
28 <https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/> (last visited April
13, 2020).

1 Such fraud may go undetected until debt collection calls commence months, or even years,
2 later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax
3 returns, file for unemployment benefits, or apply for a job using a false identity. Each of
4 these fraudulent activities is difficult to detect. An individual may not know that his or her
5 Social Security Number was used to file for unemployment benefits until law enforcement
6 notifies the individual's employer of the suspected fraud. Fraudulent tax returns are
7 typically discovered only when an individual's authentic tax return is rejected.

8 42. Moreover, it is not an easy task to change or cancel a stolen Social Security
9 Number. An individual cannot obtain a new Social Security Number without significant
10 paperwork and evidence of actual misuse. Even then, a new Social Security Number may
11 not be effective, as "[t]he credit bureaus and banks are able to link the new number very
12 quickly to the old number, so all of that old bad information is quickly inherited into the
13 new Social Security number."²⁴

14 43. This data, as one would expect, demands a much higher price on the black
15 market. Martin Walter, senior director at cybersecurity firm RedSeal, explained,
16 "[c]ompared to credit card information, personally identifiable information and Social
17 Security numbers are worth more than 10x on the black market."²⁵ As explained above, the
18 inclusion of PHI, such as the information exposed here, is even more valuable.

19 44. At all relevant times, Magellan knew, or reasonably should have known, of
20 the importance of safeguarding PII and of the foreseeable consequences if their data security
21
22

23
24 ²⁴ *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Brian
25 Naylor, Feb. 9, 2015, available at <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft> (last visited April 23, 2020).

26 ²⁵ *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*,
27 IT World, Tim Greene, Feb. 6, 2015, available at
28 <http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited April 23, 2020).

1 systems were breached, including, the significant costs that would be imposed on patients
2 as a result of a breach.

3 ***F. Magellan’s Conduct Violates HIPAA and Evidences Their Insufficient Data***
4 ***Security***

5 45. HIPAA requires covered entities to protect against reasonably anticipated
6 threats to the security of sensitive patient health information entities must implement
7 safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must
8 include physical, technical, and administrative components.²⁶

9 46. Title II of HIPAA contains what are known as the Administrative
10 Simplification provisions. 42 U.S.C. §§ 1301, *et seq.* These provisions require, among other
11 things, that the Department of Health and Human Services (“HHS”) create rules to
12 streamline the standards for handling PII like the data Defendants left unguarded. The HHS
13 has subsequently promulgated five rules under authority of the Administrative
14 Simplification provisions of HIPAA.

15 47. Defendants’ Data Breach resulted from a combination of insufficiencies that
16 demonstrate they failed to comply with safeguards mandated by HIPAA regulations.
17 Magellan’s security failures include, but are not limited to:

- 18 a. Failing to ensure the confidentiality and integrity of electronic
19 protected health information that Defendants create, receive,
20 maintain, and transmit, in violation of 45 C.F.R. § 164.306(a)(1);
21 b. Failing to implement technical policies and procedures for electronic
22 information systems that maintain electronically protected health
23 information to allow access only to those persons or software
24
25

26
27 ²⁶ *What is Considered Protected Health Information Under HIPAA?*, HIPAA Journal, April
28 22, 2018, <https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/> (last visited April 23, 2020).

- 1 programs that have been granted access rights, in violation of 45
2 C.F.R. § 164.312(a)(1);
- 3 c. Failing to implement policies and procedures to prevent, detect,
4 contain, and correct security violations, in violation of 45 C.F.R. §
5 164.308(a)(1);
- 6 d. Failing to identify and respond to suspected or known security
7 incidents and to mitigate, to the extent practicable, harmful effects of
8 security incidents that are known to the covered entity, in violation
9 of 45 C.F.R. § 164.308(a)(6)(ii);
- 10 e. Failing to protect against any reasonably anticipated threats or
11 hazards to the security or integrity of electronically protected health
12 information, in violation of 45 C.F.R. § 164.306(a)(2);
- 13 f. Failing to protect against any reasonably anticipated uses or
14 disclosures of electronically protected health information that are not
15 permitted under the privacy rules regarding individually identifiable
16 health information, in violation of 45 C.F.R. § 164.306(a)(3);
- 17 g. Failing to ensure compliance with HIPAA security standard rules by
18 their workforce, in violation of 45 C.F.R. § 164.306(a)(94);
- 19 h. Impermissibly and improperly using and disclosing protected health
20 information that is and remains accessible to unauthorized persons,
21 in violation of 45 C.F.R. §§ 164.502, *et seq.*;
- 22 i. Failing to effectively train all members of their workforce (including
23 independent contractors) on the policies and procedures with respect
24 to protected health information as necessary and appropriate for the
25 members of their workforce to carry out their functions and to
26 maintain security of protected health information, in violation of 45
27 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and
28

- 1 j. Failing to design, implement, and enforce policies and procedures
2 establishing physical and administrative safeguards to reasonably
3 safeguard protected health information, in violation of 45 C.F.R. §
4 164.530(c).

5 ***G. Magellan Failed to Comply with FTC Guidelines, Further Evidencing Their***
6 ***Insufficient Data Security***

7 48. The Federal Trade Commission (“FTC”) has promulgated numerous guides
8 for businesses which highlight the importance of implementing reasonable data security
9 practices. According to the FTC, the need for data security should be factored into all
10 business decision-making.²⁷

11 49. In 2016, the FTC updated its publication, *Protecting Personal Information:*
12 *A Guide for Business*, which established cyber-security guidelines for businesses.²⁸ The
13 guidelines note that businesses should protect the personal customer information that they
14 keep; properly dispose of personal information that is no longer needed; encrypt information
15 stored on computer networks; understand their network’s vulnerabilities; and implement
16 policies to correct any security problems.

17 50. The FTC further recommends that companies not maintain PHI and PII
18 longer than is needed for authorization of a transaction; limit access to sensitive data; require
19 complex passwords to be used on networks; use industry-tested methods for security;
20 monitor for suspicious activity on the network; and verify that third-party service providers
21 have implemented reasonable security measures.²⁹

24 ²⁷ Federal Trade Commission, *Start With Security*, available at
25 [https://www.ftc.gov/system/files/documents/plain-language/pdf0205-](https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf)
[startwithsecurity.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf) (last visited April 23, 2020).

26 ²⁸ Federal Trade Commission, *Protecting Personal Information: A Guide for Business*,
27 available at [https://www.ftc.gov/system/files/documents/plain-language/pdf-](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf)
[0136_proteting-personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf) (last visited April 23, 2020).

28 ²⁹ FTC, *Start With Security*, *supra* note 27.

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

7 52. Magellan failed to properly implement basic data security practices.
8 Magellan’s failure to employ reasonable and appropriate measures to protect against
9 unauthorized access to patient PHI and PII constitutes an unfair act or practice prohibited
10 by Section 5 of the FTC Act, 15 U.S.C. § 45.

11 53. Magellan was at all times fully aware of their obligation to protect the PHI
12 and PII of patients because of their position as a trusted healthcare provider. Magellan was
13 also aware of the significant repercussions that would result from their failure to do so.

14 ***H. Magellan Failed to Comply with Industry Standards***

15 54. Data exfiltrated from healthcare providers continues to be a high value target
16 among cybercriminals. In 2017, the U.S. healthcare sector experienced over 330 data
17 breaches, a number which continued to grow in 2018 (363 breaches).³⁰ The costs of
18 healthcare data breaches are among the highest across all industries, topping \$380 per stolen
19 record in 2017 as compared to the global average of \$141 per record.³¹ As a result, both the
20 government and private sector have developed industry best standards to address this
21 growing problem.

22 55. The Department of Health and Human Services’ Office for Civil Rights
23 (“DHHS”) notes that “[w]hile all organizations need to implement policies, procedures, and
24

25 ³⁰ <https://www.ntiva.com/blog/10-cybersecurity-best-practices-for-the-healthcare-industry;>
26 Identity Theft Resource Center, 2018 End of Year Data Brach Report,
27 [https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-
Aftermath_FINAL_V2_combinedWEB.pdf](https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf) (last visited April 23, 2020).

28 ³¹ *Id.*

1 technical solutions to make it harder for hackers to gain access to their systems and data,
2 this is especially important in the healthcare industry. Hackers are actively targeting
3 healthcare organizations as they store large quantities of highly sensitive and valuable data.”

4 ³² DHHS highlights several basic cybersecurity safeguards that can be implemented to
5 improve cyber resilience which require a relatively small financial investment, yet can have
6 a major impact on an organization’s cybersecurity posture including: (a) the proper
7 encryption of PHI and PII; (b) educating and training healthcare employees on how to
8 protect PHI and PII; and (c) correcting the configuration of software and network devices.

9 56. Private cybersecurity firms have also identified the healthcare sector as being
10 particularly vulnerable to cyber-attacks, both because of the value of the PHI and PII they
11 maintain and because as an industry they have been slow to adapt and respond to
12 cybersecurity threats.³³ They too have promulgated similar best practices for bolstering
13 cyber security and protecting against the unauthorized disclosure of PHI and PII.

14 57. Despite the abundance and availability of information regarding
15 cybersecurity best practices for the healthcare industry, Magellan chose to ignore them.
16 These best practices were known, or should have been known by Magellan, whose failure
17 to heed and properly implement them directly led to the Data Breach and the unlawful
18 exposure of PHI and PII.

19 ***I. Plaintiff and Class Members Suffered Damages***

20 58. The ramifications of Defendants’ failure to keep Patients’ PHI and PII secure
21 are long lasting and severe. Once PHI and PII is stolen, fraudulent use of that information
22
23

24 ³² *Cybersecurity Best Practices for Healthcare Organizations*, HIPAA Journal, November
25 1, 2018, <https://www.hipaajournal.com/important-cybersecurity-best-practices-for-healthcare-organizations/> (last visited April 23, 2020).

26 ³³ See, e.g., <https://www.ntiva.com/blog/10-cybersecurity-best-practices-for-the-healthcare-industry;>
27 <https://resources.infosecinstitute.com/category/healthcare-information-security/is-best-practices-for-healthcare/10-best-practices-for-healthcare-security/#gref> (last visited April 23, 2020).
28

1 and damage to victims may continue for years. Consumer victims of data breaches are more
2 likely to become victims of identity fraud.³⁴

3 59. The PII belonging to Plaintiff and Class Members is private, sensitive in
4 nature, and was left inadequately protected by Defendants, who did not obtain Plaintiff's or
5 Class Members' consent to disclose such PHI and PII to any other person as required by
6 applicable law and industry standards.

7 60. Upon receiving the Notice, Ms. Dearing immediately contacted all three
8 credit bureaus in order to put freezes on her credit. She also contacted two credit card
9 companies with whom she transacts to notify them of the breach, one of which issued her a
10 new card.

11 61. Since the announcement of the Data Breach, Ms. Dearing continues to
12 monitor her accounts in an effort to detect and prevent any misuses of her personal
13 information.

14 62. Ms. Dearing has spent and continues to spend her valuable time to protect
15 the integrity of her medical information, finances, and credit—time which she would not
16 have had to expend but for the Data Breach.

17 63. Ms. Dearing suffered actual injury from having her PHI and PII exposed as
18 a result of the Data Breach, including, but not limited to: (a) conferring and/or causing to be
19 conferred monies to Magellan that would not have been paid to Magellan had Magellan
20 disclosed that they lacked data security practices adequate to safeguard consumers' PHI and
21 PII from theft; (b) damages to and diminution in the value of her PHI and PII—a form of
22 intangible property that the Plaintiff entrusted to Magellan as a condition for health related
23 services; (c) imminent and impending injury arising from the increased risk of fraud and
24 identity theft.; and (d) the time and money she spent monitoring her accounts, contacting
25

26
27 ³⁴ 2014 LexisNexis True Cost of Fraud Study,
28 <https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf> (last visited
April 23, 2020).

1 credit bureaus and credit card companies, and otherwise attempting to protect her
2 information.

3 64. As a result of the Data Breach, Ms. Dearing will continue to be at heightened
4 risk for financial fraud, medical fraud, identity theft, and their attendant damages for years
5 to come.

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

13 66. Defendants had the resources necessary to prevent the Data Breach, but
14 neglected to adequately invest in data security measures, despite their obligations to protect
15 patient.

16 67. As a direct and proximate result of Defendants' wrongful actions and
17 inactions, Plaintiff and Class Members have been placed at an imminent, immediate, and
18 continuing increased risk of harm from identity theft and fraud, requiring them to take the
19 time which they otherwise would have dedicated to other life demands such as work and
20 family in an effort to mitigate the actual and potential impact of the Data Breach on their
21 lives. The U.S. Department of Justice's Bureau of Justice Statistics found that "among
22 victims who had personal information used for fraudulent purposes, 29% spent a month or
23 more resolving problems" and that "resolving the problems caused by identity theft [could]
24 take more than a year for some victims."³⁵

25
26
27 ³⁵ U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics,
28 *Victims of Identity Theft, 2012*, December 2013, available at
<https://www.bjs.gov/content/pub/pdf/vit12.pdf> (last visited April 13, 2019).

1 68. To date, Magellan has offered only a year of identity monitoring services to
2 a subset of affected patients. This is wholly inadequate as it fails to provide for the fact that
3 victims of data breaches and other unauthorized disclosures commonly face multiple years
4 of ongoing identity theft, medical and financial fraud and it entirely fails to provide any
5 compensation for the unauthorized release and disclosure of Plaintiff's and Class Members'
6 PII.

7 69. As a result of the Defendants' failures to prevent the Data Breach, Plaintiff
8 and Class Members have suffered, will suffer, or are at increased risk of suffering:

- 9 a. The compromise, publication, theft, and/or unauthorized use of their
10 PII;
- 11 b. Out-of-pocket costs associated with the prevention, detection,
12 recovery, and remediation from identity theft or fraud;
- 13 c. Lost opportunity costs and lost wages associated with efforts
14 expended and the loss of productivity from addressing and
15 attempting to mitigate the actual and future consequences of the Data
16 Breach, including but not limited to efforts spent researching how to
17 prevent, detect, contest, and recover from identity theft and fraud;
- 18 d. The continued risk to their PHI and PII, which remains in the
19 possession of Defendants and is subject to further breaches so long
20 as Defendants fail to undertake appropriate measures to protect the
21 PHI and PII in their possession; and
- 22 e. Current and future costs in terms of time, effort, and money that will
23 be expended to prevent, detect, contest, remediate, and repair the
24 impact of the Data Breach for the remainder of the lives of Plaintiff
25 and Class Members.

1 70. In addition to a remedy for the economic harm, Plaintiff and the Class
2 maintain an undeniable interest in ensuring that their PHI and PII is secure, remains secure,
3 and is not subject to further misappropriation and theft.

4 ***J. Defendants' Delay in Identifying and Reporting the Data Breach Caused***
5 ***Additional Harm***

6 71. It is axiomatic that “[t]he quicker a financial institution, credit card issuer,
7 wireless carrier or other service provider is notified that fraud has occurred on an account,
8 the sooner these organizations can act to limit the damage. Early notification can also help
9 limit the liability of a victim in some cases, as well as allow more time for law enforcement
10 to catch the fraudsters in the act.”³⁶

11 72. Indeed, once a data breach has occurred, “[o]ne thing that does matter is
12 hearing about a data breach quickly. That alerts consumers to keep a tight watch on credit
13 card bills and suspicious emails. It can prompt them to change passwords and freeze credit
14 reports. And notifying officials can help them catch cybercriminals and warn other
15 businesses of emerging dangers. If consumers don’t know about a breach because it wasn’t
16 reported, they can’t take action to protect themselves” (internal citations omitted).³⁷

17 73. Although their PII was improperly exposed in May 2019, Defendants did not
18 discover the Data Breach until July, and affected patients were not notified of the Data
19 Breach until November, depriving them of the ability to promptly mitigate potential adverse
20 consequences resulting from the Data Breach.

21
22
23 ³⁶ *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent*
24 *According to New Javelin Strategy & Research Study*, Business Wire,
25 [https://www.businesswire.com/news/home/20170201005166/en/Identity-Fraud-Hits-](https://www.businesswire.com/news/home/20170201005166/en/Identity-Fraud-Hits-Record-High-15.4-Million)
Record-High-15.4-Million (last visited April 23, 2020).

26 ³⁷ *The Data Breach Next Door Security breaches don't just hit giants like Equifax and*
27 *Marriott. Breaches at small companies put consumers at risk, too*, Consumer Reports,
28 January 31, 2019, <https://www.consumerreports.org/data-theft/the-data-breach-next-door/>
(last visited April 23, 2020).

- c. Whether Magellan’s security measures to protect their systems were reasonable in light of best practices recommended by data security experts;
- d. Whether Magellan was negligent in failing to implement reasonable and adequate security procedures and practices;
- e. Whether Magellan’s failure to implement adequate data security measures allowed the breach of their data systems to occur;
- f. Whether Magellan’s conduct, including their failure to act, resulted in or was the proximate cause of the breach of their systems, resulting in the unlawful exposure of the Plaintiff’ and Class Members’ PHI and PII;
- g. Whether Plaintiff and Class Members were injured and suffered damages or other losses because of Magellan’s failure to reasonably protect their systems and data network; and,
- h. Whether Plaintiff and Class members are entitled to relief.

81. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Rule 23(a)(3), Plaintiff’s claims are typical of those of other Class Members. Plaintiff was a Magellan member patient whose PII was exposed in the Data Breach. Plaintiff’s damages and injuries are akin to other Class Members, and Plaintiff seeks relief consistent with the relief sought by the Class.

82. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class she seeks to represent; is committed to pursuing this matter against Magellan to obtain relief for the Class; and has no conflicts of interest with the Class. Moreover, Plaintiff’s Counsel are competent and experienced in litigating class actions, including privacy litigation of this kind. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class’s interests.

1 83. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class
2 action is superior to any other available means for the fair and efficient adjudication of this
3 controversy, and no unusual difficulties are likely to be encountered in the management of
4 this class action. The quintessential purpose of the class action mechanism is to permit
5 litigation against wrongdoers even when damages to an individual plaintiff may not be
6 sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the
7 Class are relatively small compared to the burden and expense required to individually
8 litigate their claims against Magellan, and thus, individual litigation to redress Magellan's
9 wrongful conduct would be impracticable. Individual litigation by each Class Member
10 would also strain the court system. Individual litigation creates the potential for
11 inconsistent or contradictory judgments and increases the delay and expense to all parties
12 and the court system. By contrast, the class action device presents far fewer management
13 difficulties and provides the benefits of a single adjudication, economies of scale, and
14 comprehensive supervision by a single court.

15 84. **Injunctive and Declaratory Relief.** Class certification is also appropriate
16 under Rule 23(b)(2) and (c). Defendant, through their uniform conduct, acted or refused to
17 act on grounds generally applicable to the Class as a whole, making injunctive and
18 declaratory relief appropriate to the Class as a whole.

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

- 23 a. Whether Magellan failed to timely notify the public of the Data
24 Breach;
- 25 b. Whether Magellan owed a legal duty to Plaintiff and the Class to
26 exercise due care in collecting, storing, and safeguarding their PHI
27 and PII;

- c. Whether Magellan’s security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;
- d. Whether Defendants’ failure to institute adequate protective security measures amounted to negligence;
- e. Whether Defendants failed to take commercially reasonable steps to safeguard patient PHI and PII;
- f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have
- g. reasonably prevented the data breach; and
- h. Whether Magellan failed to comply with their obligations under HIPAA.

86. Finally, all members of the proposed Class are readily ascertainable. Magellan has access to patient names and addresses affected by the Data Breach. Using this information, Class Members can be identified and ascertained for the purpose of providing notice.

FIRST CAUSE OF ACTION
NEGLIGENCE

87. Plaintiff restates and realleges the paragraphs 1 through 86 as if fully set forth herein.

88. As a condition of receiving services, Plaintiff and Class Members were obligated to provide Magellan directly, or through their respective insurance providers, with their PHI and PII.

89. Plaintiff and the Class Members entrusted their PHI and PII to Magellan with the understanding that Magellan would safeguard their information.

90. Defendants had full knowledge of the sensitivity of the PHI and PII and the types of harm that Plaintiff and Class Members could and would suffer if the PHI and PII were wrongfully disclosed.

1 91. Defendants had a duty to exercise reasonable care in safeguarding, securing
2 and protecting such information from being compromised, lost, stolen, misused, and/or
3 disclosed to unauthorized parties. This duty includes, among other things, designing,
4 maintaining, and testing the Defendants' security protocols to ensure that PHI and PII in
5 their possession was adequately secured and protected and that employees tasked with
6 maintaining such information were adequately training on cyber security measures
7 regarding the security of such information.

8 92. Plaintiff and the Class Members were the foreseeable and probable victims
9 of any inadequate security practices and procedures. Defendants knew of or should have
10 known of the inherent risks in collecting and storing the PHI and PII of Plaintiff and the
11 Class, the critical importance of providing adequate security of that PII, the current cyber
12 scams being perpetrated, and that they had inadequate employee training and education and
13 IT security protocols in place to secure the PHI and PII of Plaintiff and the Class.

14 93. Defendants' own conduct created a foreseeable risk of harm to Plaintiff and
15 Class Members. Defendants' misconduct included, but was not limited to, their failure to
16 take the steps and opportunities to prevent the Data Breach as set forth herein. Defendants'
17 misconduct also included their decision not to comply with HIPAA and industry standards
18 for the safekeeping and encrypted authorized disclosure of the PHI and PII of Plaintiff and
19 Class Members.

20 94. Plaintiff and the Class Members had no ability to protect their PHI and PII
21 that was in Magellan's possession.

22 95. Defendants were in a position to protect against the harm suffered by
23 Plaintiff and Class Members as a result of the Data Breach.

24 96. Defendants had a duty to put proper procedures in place in order to prevent
25 the unauthorized dissemination of Plaintiff's and Class Members' PHI and PII.

26 97. Defendants admitted that Plaintiff's and Class Members' PII was wrongfully
27 disclosed to unauthorized third persons as a result of the Data Breach.

28

1 98. Defendants, through their actions and/or omissions, unlawfully breached
2 their duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting
3 and safeguarding the Plaintiff's and Class Members' PHI and PII while it was within the
4 Magellan's possession or control.

5 99. Defendants improperly and inadequately safeguarded Plaintiff's and Class
6 Members' PHI and PII in deviation of standard industry rules, regulations and practices at
7 the time of the Data Breach.

8 100. Defendants, through their actions and/or omissions, unlawfully breached
9 their duty to Plaintiff and Class Members by failing to have appropriate procedures in place
10 to detect and prevent dissemination of their patients' PHI and PII.

11 101. Defendants, through their actions and/or omissions, unlawfully breached
12 their duty to timely and adequately disclose to Plaintiff and Class Members the existence,
13 and scope of the Data Breach.

14 102. But for Defendants' wrongful and negligent breach of duties owed to
15 Plaintiff and Class Members, Plaintiff's and Class Members' PHI and PII would not have
16 been compromised.

17 103. There is a temporal and close causal connection between Defendants' failure
18 to implement security measures to protect the PII and the harm suffered, or risk of imminent
19 harm suffered by Plaintiff and the Class.

20 104. As a result of Defendants' negligence, Plaintiff and the Class Members have
21 suffered and will continue to suffer damages and injury including, but not limited to: out-
22 of-pocket expenses associated with procuring robust identity protection and restoration
23 services; increased risk of future identity theft and fraud, and the costs associated therewith;
24 time spent monitoring, addressing, and correcting the current and future consequences of
25 the Data Breach; and the necessity to engage legal counsel and incur attorneys' fees, costs
26 and expenses.

27 //

28

SECOND CAUSE OF ACTION
NEGLIGENCE PER SE

1
2
3 105. Plaintiff restates and realleges paragraphs 1 through 86 as if fully set forth
4 herein.

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

10 107. Magellan violated Section 5 of the FTC Act by failing to use reasonable
11 measures to protect patient PII and not complying with applicable industry standards, as
12 described in detail herein. Magellan’s conduct was particularly unreasonable given the
13 nature and amount of PII they obtained and stored, and the foreseeable consequences of a
14 data breach including, specifically, the damages that would result to Plaintiff and Class
15 Members.

16 108. Magellan’s violation of Section 5 of the FTC Act constitutes negligence per
17 se.

18 109. Plaintiff and Class Members are within the class of persons that the FTC Act
19 was intended to protect.

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

25 111. As a direct and proximate result of Magellan’s negligence per se, Plaintiff
26 and the Class have suffered, and continue to suffer, injuries and damages arising from the
27 Data Breach including, but not limited to: damages from lost time and effort to mitigate the
28 actual and potential impact of the Data Breach on their lives, including, *inter alia*, by placing

1 “freezes” and “alerts” with credit reporting agencies; contacting their financial institutions;
2 closing or modifying financial and medical accounts; closely reviewing and monitoring
3 their credit reports and various accounts for unauthorized activity and filing police reports;
4 and damages from identity theft, which may take months if not years to discover and detect.

5 112. Additionally, as a direct and proximate result of Magellan’s negligence per
6 se, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure
7 of their PII, which remain in Magellan’s possession and is subject to further unauthorized
8 disclosures so long as Magellan fails to undertake appropriate and adequate measures to
9 protect the PII in their continued possession.

10 **THIRD CAUSE OF ACTION**
11 **BREACH OF IMPLIED CONTRACT**

12 113. Plaintiff restates and realleges paragraphs 1 through 86 as if fully set forth
13 herein.

14 114. Plaintiff and Class Members were required to provide their PII, including
15 their names, Social Security numbers, addresses, medical record numbers, dates of birth,
16 telephone numbers, email addresses, and various health related information to Defendants
17 as a condition of their use of Defendants’ services.

18 115. Plaintiff and Class Members paid money, or money was paid on their behalf,
19 to Defendants in exchange for services, along with Defendants’ promise to protect their
20 health information and other PII from unauthorized disclosure.

21 116. In their written privacy policies, Magellan expressly promised Plaintiff and
22 Class Members that they would only disclose PHI and other PII under certain circumstances,
23 none of which relate to the Data Breach.

24 117. Magellan promised to comply with HIPAA standards and to make sure that
25 Plaintiff’s and Class Members’ PHI and other PII would remain protected.

26 118. Implicit in the agreement between Plaintiff and Class Members and the
27 Defendants to provide PHI and other PII, was the latter’s obligation to: (a) use such PHI and
28 PII for business purposes only; (b) take reasonable steps to safeguard that PHI and PII; (c)

1 prevent unauthorized disclosures of the PHI and PII; (d) provide Plaintiff and Class
2 Members with prompt and sufficient notice of any and all unauthorized access and/or theft
3 of their PHI and PII; (e) reasonably safeguard and protect the PHI and PII of Plaintiff and
4 Class Members from unauthorized disclosure or uses; and (f) retain the PHI and PII only
5 under conditions that kept such information secure and confidential.

6 119. Without such implied contracts, Plaintiff and Class Members would not have
7 provided their PHI and PII to Defendants.

8 120. Plaintiff and Class Members fully performed their obligations under the
9 implied contract with Defendants, however, Defendants did not.

10 121. Defendants breached the implied contracts with Plaintiff and Class Members
11 by failing to, *inter alia*:

- 12 a. Reasonably safeguard and protect Plaintiff's and Class Members'
13 PHI and PII, which was compromised as a result of the Data Breach;
- 14 b. Comply with their promise to abide by HIPAA;
- 15 c. Ensure the confidentiality and integrity of electronic protected health
16 information Defendants created, received, maintained, and
17 transmitted, in violation of 45 C.F.R. § 164.306(a)(1);
- 18 d. Implement technical policies and procedures for electronic
19 information systems that maintain electronically PHI to allow access
20 only to those persons or software programs that have been granted
21 access rights, in violation of 45 C.F.R. § 164.312(a)(1);
- 22 e. Implement policies and procedures to prevent, detect, contain, and
23 correct security violations, in violation of 45 C.F.R. § 164.308(a)(1);
- 24 f. Identify and respond to suspected or known security incidents;
25 mitigate, to the extent practicable, harmful effects of security
26 incidents that are known to the covered entity, in violation of 45
27 C.F.R. § 164.308(a)(6)(ii); and
28

1 g. Protect against any reasonably anticipated threats or hazards to the
2 security or integrity of electronic protected health information, in
3 violation of 45 C.F.R. § 164.306(a)(2).

4 **FOURTH CAUSE OF ACTION**
5 **UNJUST ENRICHMENT**

6 122. Plaintiff restates and realleges paragraphs 1 through 86 as if fully set forth
7 herein.

8 123. Plaintiff and Class Members conferred a monetary benefit on Defendants.
9 Specifically, they purchased goods and services from Defendants and, in so doing, provided
10 Defendants with their PHI and PII. In exchange, Plaintiff and Class Members should have
11 received from Defendants the goods and services that were the subject of the transaction
12 and have their PHI and PII protected with adequate data security.

13 124. Defendants knew that Plaintiff and Class Members conferred a benefit which
14 Defendants accepted. Defendants profited from these transactions and used the PHI and PII
15 of Plaintiff and Class Members for business purposes.

16 125. The amounts Plaintiff and Class Members paid for goods and services were
17 used, in part, to pay for use of Defendants' network and the administrative costs of data
18 management and security.

19 126. Under the principles of equity and good conscience, Defendants should not
20 be permitted to retain the money belonging to Plaintiff and Class Members, because
21 Defendants failed to implement appropriate data management and security measures that
22 are mandated by industry standards.

23 127. Defendants failed to secure Plaintiff's and Class Members' PHI and PII and,
24 therefore, did not provide full compensation for the benefit Plaintiff and Class Members
25 provided.

26 128. Defendants acquired the PHI and PII through inequitable means in that it
27 failed to disclose the inadequate security practices previously alleged.
28

1 129. If Plaintiff and Class Members knew that Defendants had not secured their
2 PHI and PII, they would not have agreed to Defendants' services.

3 130. Plaintiff and Class Members have no adequate remedy at law.

4 131. As a direct and proximate result of Defendants' conduct, Plaintiff and Class
5 Members have suffered and will suffer injury, including but not limited to: (i) actual identity
6 theft; (ii) the loss of the opportunity how their PHI and PII is used; (iii) the compromise,
7 publication, and/or theft of their PHI and PII; (iv) out-of-pocket expenses associated with
8 the prevention, detection, and recovery from identity theft, and/or unauthorized use of their
9 PHI and PII; (v) lost opportunity costs associated with effort expended and the loss of
10 productivity addressing and attempting to mitigate the actual and future consequences of
11 the Data Breach, including but not limited to efforts spent researching how to prevent,
12 detect, contest, and recover from identity theft; (vi) the continued risk to their PHI and PII,
13 which remain in Defendants' possession and is subject to further unauthorized disclosures
14 so long as Defendants fails to undertake appropriate and adequate measures to protect PHI
15 and PII in their continued possession; and (vii) future costs in terms of time, effort, and
16 money that will be expended to prevent, detect, contest, and repair the impact of the PHI
17 and PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff
18 and Class Members.

19 132. As a direct and proximate result of Defendants' conduct, Plaintiff and Class
20 Members have suffered and will continue to suffer other forms of injury and/or harm.

21 133. Defendants should be compelled to disgorge into a common fund or
22 constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly
23 received from them. In the alternative, Defendants should be compelled to refund the
24 amounts that Plaintiff and Class Members overpaid for Defendants' services.

25 //

26 //

27 //

28

FIFTH CAUSE OF ACTION
ARIZONA CONSUMER FRAUD ACT (“ACFA”)
Ariz. Rev. Stat. §§ 44-1521, et seq.

134. Plaintiff restates and realleges paragraphs 1 through 86 as if fully set forth herein.

135. 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 fact been misled, deceived or damaged thereby, is declared to be an unlawful practice.

Id. § 44-1522.

136. Plaintiff and Class Members are “persons” as defined by Ariz. Rev. Stat. § 44-1521(6), Magellan provides “services” as that term is included in the definition of “merchandise” under Ariz. Rev. Stat. § 44-1521(5), and Magellan is engaged in the “sale” of “merchandise” as defined by Ariz. Rev. Stat. § 44-1521(7).

137. Magellan 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 Plaintiff’s 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

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

- 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 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 Magellan Data Breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws;
 - g. Engaging in unlawful, unfair, and deceptive acts and practices with respect to the sale of health benefit services by failing to disclose the Magellan 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.

1 138. The above unlawful, unfair, and deceptive acts and practices by Magellan
2 were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury
3 to Plaintiff and Class Members that they could not reasonably avoid; this substantial injury
4 outweighed any benefits to consumers or to competition.

5 139. Magellan knew or should have known that their computer systems and data
6 security practices were inadequate to safeguard Class Members' PHI and PII and that risk
7 of a data breach or theft was high. Magellan's actions in engaging in the above-named
8 deceptive acts and practices were negligent, knowing and willful, and/or wanton and
9 reckless with respect to the rights of Members of the Class.

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

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

17 **SIXTH CAUSE OF ACTION**
18 **INJUNCTIVE AND DECLARATORY RELIEF**

19 142. Plaintiff restates and realleges paragraphs 1 through 86 as if fully set forth
20 herein

21 143. Plaintiffs seek a declaration that: (i) Magellan's existing data security
22 measures do not comply with its contractual obligations and duties of care; and (ii) in order
23 to comply with its contractual obligations and duties of care, Magellan must implement and
24 maintain reasonable security measures, including, but not limited to:

- 25 a. Engaging third-party security auditors/penetration testers as well as
26 internal security personnel to conduct testing, including simulated
27 attacks, penetration tests and audits on Magellan's systems on a
28

- 1 periodic basis, and ordering Magellan to promptly correct any
2 problems or issues detected by such third-party security auditors;
- 3 b. Engaging third-party security auditors and internal personnel to run
4 automated security monitoring;
- 5 c. Auditing, testing and training their security personnel regarding any
6 new or modified procedures;
- 7 d. Segmenting customer data by, among other things, creating firewalls
8 and access controls so that if one area of Magellan is compromised,
9 hackers cannot gain access to other portions of Magellan's systems;
- 10 e. Purging, deleting and destroying PII and PHI not necessary for its
11 provisions of services in a reasonably secure manner;
- 12 f. Conducting regular database scans and security checks;
- 13 g. Routinely and continually conducting internal training and education
14 to inform internal security personnel how to identify and contain a
15 breach when it occurs and what to do in response to a breach; and
- 16 h. Educating its members and their beneficiaries about the threats they
17 face as a result of the loss of their financial and personal information
18 to third parties, as well as the steps they should take to protect
19 themselves.

20 144. As a direct result of Magellan's knowing violations of HIPAA, the FTCA
21 and industry standards, Class Members are entitled to a declaration that: (i) Magellan's
22 existing data security measures do not comply with the requirements imposed upon it by
23 law; and (ii) in order to comply with its legal obligations and duties of care, Magellan must
24 implement and maintain reasonable security measures, including but not limited to,
25 injunctive relief:

- 26 a. Ordering that Magellan engage third-party security
27 auditors/penetration testers as well as internal security personnel to
28

1 conduct testing, including simulated attacks, penetration tests, and
2 audits on systems on a periodic basis, and ordering Magellan to
3 promptly correct any problems or issues detected by such third-party
4 security auditors;

5 b. Ordering that Magellan engage third-party security auditors and
6 internal personnel to run automated security monitoring;

7 c. Ordering that Magellan audit, test and train its security personnel
8 regarding any new or modified procedures;

9 d. Ordering that Magellan segment PII and PHI by, among other things,
10 creating firewalls and access controls so that if one area is
11 compromised, hackers cannot gain access to other portions of
12 Magellan's systems;

13 e. Ordering that Magellan purge, delete and destroy PII and PHI not
14 necessary for its provisions of services in a reasonably secure
15 manner;

16 f. Ordering that Magellan conduct regular database scans and security
17 checks;

18 g. Ordering that Magellan routinely and continually conduct internal
19 training and education to inform internal security personnel how to
20 identify and contain a breach when it occurs and what to do in
21 response to a breach; and

22 h. Ordering Magellan to meaningfully educate its members and their
23 beneficiaries about the threats they face as a result of the loss of their
24 financial and personal information to third parties, as well as the steps
25 they should take to protect themselves.

26 145. Absent injunctive and declaratory relief, Plaintiff and Class Members' PHI
27 and PII, which Defendants possess, continues to be at risk of further breaches.

1 **WHEREFORE**, Plaintiff, on behalf of herself and all others similarly situated,
2 respectfully requests the following relief:

- 3 a. An Order certifying this case as a class action;
- 4 b. An Order appointing Plaintiff as the class representative;
- 5 c. An Order appointing undersigned counsel as class counsel;
- 6 d. An Order compelling Defendants to disgorge into a common fund or
7 constructive trust, for the benefit of Plaintiff and Class Members,
8 proceeds that they unjustly received from them or, alternatively,
9 compelling Defendants to refund the amounts that Plaintiff and Class
10 Members overpaid for Defendants' services;
- 11 e. A mandatory injunction directing the Defendants to hereinafter
12 adequately safeguard the PHI and PII of Plaintiff and the Class by
13 implementing improved security procedures and measures;
- 14 f. An award of damages;
- 15 g. An award of costs and expenses;
- 16 h. An award of attorneys' fees; and
- 17 i. Such other and further relief as this court may deem just and proper.

18 **DEMAND FOR JURY TRIAL**

19 Plaintiff demands a jury trial as to all issues triable by a jury.

20
21 DATED this 17th day of April 2020.

22
23 BONNETT, FAIRBOURN, FRIEDMAN
& BALINT, P.C.
24 By Carrie A. Laliberte

25 Carrie A. Laliberte (AZ Bar #032556)
26 Elaine A. Ryan (AZ Bar #012870)
27 2325 E. Camelback Rd., Suite 300
Phoenix AZ 85016
Telephone: (602) 274-1100
eryan@bffb.com
28 claliberte@bffb.com

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

Patricia N. Syverson (AZ Bar #020191)
BONNETT, FAIRBOURN, FRIEDMAN
& BALINT, P.C.
600 W. Broadway, Suite 900
San Diego, California 92101
Telephone: (619) 798-4593
psyverson@bffb.com

As local counsel for:

John A. Yanchunis*
Patrick A. Barthle*
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
jyanchunis@forthepeople.com
pbarthle@forthepeople.com

Joel R. Rhine*
Martin A. Ramey*
Chris B. Barbour*
RHINE LAW FIRM, P.C.
1612 Military Cutoff Road, Suite 300
Wilmington, NC 28403
Telephone: (910) 772-9960
jrr@rhinelawfirm.com
mjr@rhinelawfirm.com

Counsel for Plaintiff and the Putative
Class

*Motions for *pro hac vice* admission
to be filed

EXHIBIT A

MagellanRx MANAGEMENTSM

C/O ID Experts
PO Box 4219
Everett WA 98204

To Enroll, Please Call:
(833) 959-1351
Or Visit:
<https://ide.myidcare.com/magellanhealthcare-nia-protect>
Enrollment Code: [REDACTED]

*****AUTO**5-DIGIT 388
[REDACTED]



November 8, 2019

Re: Notice of Possible Data Breach

Dear Carol Dearing:

Magellan Rx Management, a subsidiary of Magellan Health, Inc. ("Magellan"), manages the pharmacy benefits for TennCare and its members. We review health care services to make sure they are medically necessary and should be paid.

This letter is to let you know that some information about you may have been put at risk.

What Happened

On July 5th, 2019, Magellan learned that one of our employee's email accounts had been hacked by an unknown third party ("hacker") on May 28th, 2019. Our Information Security team immediately took steps to lock down this employee's account and make sure no others could access it. We also immediately undertook an investigation to find out if any other email accounts were hacked. We believe that the hacker was trying to access our employee's email account to send out spam. Spam is unwanted email from unknown people. We also believe he or she had no plan to view, read or do anything with the emails. We cannot say for sure that no emails were seen. While we have no proof that the hacker saw any emails, we are being extra careful. We want you to know that your information was in at least one email.

What Information Was Involved

We understand you may be worried about this. The emails that may have been seen had information such as:

- Your name
- Your Social Security Number
- Your health plan member ID number
- The name of your health plan
- Your provider
- Drug name

What You Can Do

While we do not know of any attempt by the hacker to access or use your personal information, we are offering you services through ID Experts®, the data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare services include: 12 months of Credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling 833-959-1351 or going to <https://ide.myidcare.com/magellanhealthcare-nia-protect> and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is February 8, 2020. You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling on online.

Also:

1. Website and Enrollment. Go to <https://ide.myidcare.com/magellanhealthcare-nia-protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your MyIDCare membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

3. Telephone. Contact MyIDCare at (833) 959-1351 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (<http://www.ca.gov/Privacy>) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center
Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone:
877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.rtag.ri.gov,
Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580,
www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

Re: Aviso de posible violación de información

Estimado/a Carol Dearing:

Magellan Rx Management, una subsidiaria de Magellan Health, Inc. ("Magellan"), administra los beneficios de farmacia para TennCare y sus miembros. Revisamos los servicios de atención médica para asegurarnos de que sean médicamente necesarios y de que deban pagarse.

Esta carta es para informarle que cierta información suya podría haber sido puesta en riesgo.

¿Qué ocurrió?

El 5 de julio de 2019, Magellan se enteró de que una de las cuentas de correo electrónico de nuestros empleados había sido hackeada por un tercero desconocido ("hacker") el 28 de mayo de 2019. Nuestro equipo de Seguridad de la información inmediatamente tomó medidas para bloquear la cuenta de este empleado y asegurarse de que nadie más pudiera acceder a ella. También realizamos una investigación de inmediato para descubrir si alguna otra cuenta de correo electrónico había sido hackeada. Creemos que el hacker estaba intentando acceder a la cuenta de correo electrónico de nuestros empleados para enviar spam. El spam es correo no deseado de personas desconocidas. También creemos que el hacker no tenía planes de ver, leer o hacer nada con los correos electrónicos. No podemos afirmar con certeza que no se hayan visto correos electrónicos. Si bien no tenemos pruebas de que el hacker haya visto ningún correo electrónico, tenemos mucho cuidado. Queremos que sepa que su información estaba en al menos un correo electrónico.

¿Qué información se vio involucrada?

Comprendemos que pueda estar preocupado por esto. Los correos electrónicos que podrían haber sido vistos tenían información como:

- Su nombre
- Su Número de seguro social
- Su número de identificación de miembro del plan de salud
- El nombre de su plan de salud
- Su proveedor
- Nombre del fármaco

¿Qué puede hacer usted?

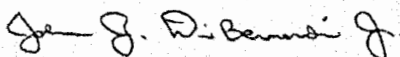
Si bien no tenemos conocimiento de ningún intento por parte del hacker de acceder o utilizar su información personal, le ofrecemos servicios a través de ID Experts®, especialista en servicios de recuperación y violación de datos, a fin de poder proporcionarle MyIDCare™. Los servicios de MyIDCare incluyen los siguientes: 12 meses de supervisión de crédito y CyberScan, una política de reembolso de \$1,000,000 en concepto de seguro y servicios de recuperación de robo de identidad completamente administrados. Con esta protección, MyIDCare lo ayudará a resolver problemas si su identidad está comprometida.

Le recomendamos que se ponga en contacto con ID Experts ante cualquier duda y que se inscriba en los servicios gratuitos de MyIDCare llamando al 833-959-1351, o bien, visitando el sitio web <https://ide.myidcare.com/magellanhealthcare-ria-protect> y utilizando el código de inscripción proporcionado anteriormente. Los especialistas de MyIDCare están disponibles de lunes a viernes, de 9 a. m. a 9 p. m., hora del este. Tenga en cuenta que la fecha límite para inscribirse es de tres meses a partir de la fecha de esta carta. Encontrará instrucciones detalladas para la inscripción en el documento adjunto Recommended Steps (Pasos recomendados). Además, deberá hacer referencia al código de inscripción en la parte superior de esta carta cuando llame o se inscriba en línea.

- Keep this letter in a safe place in case you need it later
- Review all mail from Magellan and TennCare
- If you see something wrong in what we or TennCare send you, please call the number on your ID card.

Again, at this time, there is no evidence that any of your personal information has been accessed or misused. However, we encourage you to take full advantage of the service we are offering. MyIDCare representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information. Please call 833-959-1351 or go to <https://ide.mvidcare.com/magellanhealthcare-nia-protect> for assistance or for any additional questions you may have.

Sincerely,



John J. DiBernardi, Jr.
SVP and Chief Compliance Officer

Encl.

Do you need help talking with us or reading what we send you?

Do you have a disability and need help getting care or taking part in one of our programs or services?

Or do you have more questions about your health care?

Call us for free at 1-888-816-1680. We can connect you with the free help or service you need. (For TRS call: 711)

We obey federal and state civil rights laws. We do not treat people in a different way because of their race, color, birth place, language, age, disability, religion, or sex. Do you think we did not help you or you were treated differently because of your race, color, birth place, language, age, disability, religion, or sex? You can file a complaint by mail, by e-mail, or by phone. Here are two places where you can file a complaint:

TennCare Office of Civil Rights Compliance

310 Great Circle Road, Floor 3W
Nashville, Tennessee 37243

Email: HCFA.Fairtreatment@tn.gov

Phone: 1-855-857-1673 (TRS 711)

You can get a complaint form online at:

<http://www.tn.gov/assets/entities/tenncare/attachments/complaintform.pdf>

U.S. Department of Health & Human Services Office for Civil Rights

200 Independence Ave SW, Rm 509F, HHH Bldg
Washington, DC 20201

Phone: 1-800-368-1019

(TDD): 1-800-537-7697

You can get a complaint form online at:

<http://www.hhs.gov/ocr/office/file/index.html>

Or you can file a complaint online at:

<https://ocrportal.hhs.gov/ocr/portal/lobby.jsf>

Recommended Steps to help Protect your Information

**UNITED STATES DISTRICT COURT
DISTRICT OF ARIZONA**

Civil Cover Sheet

This automated JS-44 conforms generally to the manual JS-44 approved by the Judicial Conference of the United States in September 1974. The data is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. The information contained herein neither replaces nor supplements the filing and service of pleadings or other papers as required by law. This form is authorized for use only in the District of Arizona.

The completed cover sheet must be printed directly to PDF and filed as an attachment to the Complaint or Notice of Removal.

Plaintiff
(s): **Carol Dearing**

County of Residence: Outside the State of
Arizona

County Where Claim For Relief Arose: Maricopa

Plaintiff's Atty(s):

Carrie Laliberte
Bonnett Fairbourn Friedman & Balint
2325 E Camelback Rd., #300
Phoenix, Arizona 85016
6022741100

Elaine A Ryan
Bonnett Fairbourn Friedman & Balint
2325 E Camelback Rd., #300
Phoenix, Arizona 85016
6022741100

Defendant Magellan Health Inc. ; Magellan
(s): **RX Management LLC**

County of Residence: Maricopa

Defendant's Atty(s):

II. Basis of Jurisdiction: **4. Diversity (complete item III)**

III. Citizenship of Principal
Parties (Diversity Cases Only)

Plaintiff:- **2 Citizen of Another State**
Defendant:- **4 AZ corp or Principal place of Bus. in AZ**

IV. Origin : **1. Original Proceeding**
360 Other Personal Injury

V. Nature of Suit:VI. Cause of Action: **28 USC § 1332(d). Data Breach**VII. Requested in ComplaintClass Action: **Yes**

Dollar Demand:

Jury Demand: **Yes**VIII. This case is not related to another case.

Signature: s/Carrie A. Laliberte**Date: 04/17/2020**

If any of this information is incorrect, please go back to the Civil Cover Sheet Input form using the *Back* button in your browser and change it. Once correct, save this form as a PDF and include it as an attachment to your case opening documents.

Revised: 01/2014

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Magellan Health, Rx Management Face Class Action Over May 2019 Data Breach](#)
