

Exhibit A3

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

8 Elaine A. Ryan (AZ Bar #012870)
9 Carrie A. Laliberte (AZ Bar #032556)
10 **BONNETT, FAIRBOURN, FRIEDMAN**
11 **& BALINT, P.C.**
12 2325 E. Camelback Rd., Suite 300
13 Phoenix AZ 85016
14 Telephone: (602) 274-1100
15 Email: eryl@bff.com
16 claliberte@bff.com

17 *Attorneys for Plaintiffs and the Class*
18 *(Additional Counsel listed below)*

19 **UNITED STATES DISTRICT COURT**
20 **DISTRICT OF ARIZONA**

21 Chris Griffey, et al.,
22 Plaintiffs,
23 v.
24 Magellan Health, Incorporated,
25 Defendant.

No. CV-20-01282-PHX-MTL (Lead)
No. CV-20-01350-PHX-MTL (Consol.)

CONSOLIDATED CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

(Assigned to the Honorable Michael T. Liburdi)

26 Daniel Ranson, et al.,
27 Plaintiffs,
28 v.
Magellan Health, Incorporated,
Defendant.

1 Plaintiffs Chris Griffey, Bharath Maduranthgam Rayam, Michael Domingo, Laura
2 Leather, Clara Williams, Daniel Ranson, Mitchell Flanders, Joseph Rivera, and Teresa
3 Culberson, on behalf of themselves and all others similarly situated, by and through their
4 undersigned counsel, bring this consolidated class action lawsuit against Defendant
5 Magellan Health, Inc. to obtain damages, restitution, and injunctive relief from Defendant
6 for the Class, as defined below, resulting from an April 2020 data breach (the “Data
7 Breach”), and allege, based upon information and belief, the investigation of their
8 counsel, and the facts that are a matter of public record:

9 **PARTIES**

10 1. Plaintiff Chris Griffey is, and at all times mentioned herein was, a citizen
11 of the state of Missouri residing in the city of Wildwood. Plaintiff Griffey was employed
12 by Magellan Health from December 12, 2011 through July 6, 2016. During the summer
13 of 2020, Plaintiff Griffey received notice from Magellan that the Data Breach had
14 occurred following an attack on Magellan’s computer systems. A copy of the notice is
15 attached hereto as Exhibit A.

16 2. Plaintiff Bharath Maduranthgam Rayam is, and at all times mentioned
17 herein was, a citizen of the state of Tennessee residing in the city of Nashville. Plaintiff
18 Rayam was employed by Magellan Health from March 16, 2020 through May 8, 2020.
19 Plaintiff Rayam received notice of the Data Breach, and a copy of the notice is attached
20 hereto as Exhibit B.

21 3. Plaintiff Michael Domingo is, and at all times mentioned herein was, a
22 citizen of the state of Pennsylvania residing in the city of Jamison. Plaintiff Domingo
23 was employed by Magellan Health from August 2016 through February 29, 2020.
24 Plaintiff Domingo received notice of the Data Breach, and a copy of the notice is attached
25 hereto as Exhibit C.

26 4. Plaintiff Laura Leather is, and at all times mentioned herein was, a citizen
27 of the state of New York residing in the city of Dover Plains. Upon information and
28 belief, Magellan Health provided services to her employer and/or to her health plan.

1 Plaintiff Leather received notice of the Data Breach, and a copy of the notice is attached
2 hereto as Exhibit D. As a result of the Data Breach, Plaintiff Leather has taken responsive
3 measures that she otherwise would not have taken to ensure that her identity is not stolen
4 and that her personal affairs are not further compromised.

5 5. Plaintiff Clara Williams is, and at all times mentioned herein was, a citizen
6 of the state of Arizona residing in the city of Apache Junction. Plaintiff Williams was
7 employed by Magellan Health from July of 2017 through November of 2017. While
8 employed with Magellan Health, she was a member of a health plan serviced by Magellan
9 Health. Plaintiff Williams received notice of the Data Breach, and a copy of the notice is
10 attached hereto as Exhibit E.

11 6. As a result of the Data Breach, a criminal used Plaintiff Williams' name
12 and Social Security number to apply for Arizona Unemployment Benefits. Plaintiff
13 Williams became aware of this fraud in June of 2020, when she received a letter from the
14 Arizona Department of Economic Security ("ADES") notifying her of an award of
15 benefits for which she did not apply. Plaintiff Williams thereafter contacted the ADES,
16 filed an incident report with her local police department, filed a fraud report with the
17 ADES, filed a report with the Arizona Attorney General's Office, filed a report with the
18 Federal Trade Commission, filed a report with the Federal Inspector General's Office,
19 contacted her local Social Security Office, contacted all three credit bureaus and locked
20 her credit reports, and contacted her current employer's human resource department.

21 7. Plaintiff Daniel Ranson is a citizen and resident of California. Plaintiff
22 Ranson is a licensed clinical social worker in California and currently practices as a
23 psychotherapist in Mammoth Lakes, California. At the time of the Data Breach, Plaintiff
24 had contracted with Magellan to treat behavioral health patients with Human Affairs
25 International of California ("HAIC"), a wholly owned subsidiary of Magellan Healthcare,
26 Inc., which serves as a mental health service administrator ("MHSA") for Blue Shield of
27
28

1 California, Blue Shield Life & Health Insurance Company, and other health plans.¹
2 Plaintiff Ranson received written notice of the Data Breach, and a true and correct copy
3 of that Notice is attached hereto as Exhibit F.

4 8. As a result of the Data Breach, Plaintiff Ranson enlisted the support of a
5 credit monitoring service to protect himself against the unauthorized use of his data, and
6 he changed passwords associated with his online accounts. As a health care provider
7 with a busy practice, Plaintiff Ranson has had to allot time in his schedule to review his
8 credit reports and accounts on a regular basis, scrutinizing his accounts on a level much
9 greater than before. Following the filing of his complaint in his related case, *Ranson v.*
10 *Magellan Health*, No. CV-20-01350-PHX-MTL (D. Ariz.), someone was able to
11 successfully open an account with AT&T under Ranson's name. As a direct and
12 proximate result of that fraudulent account opening, Plaintiff Ranson was required to
13 spend considerable time trying to resolve the problem – time that he could have spent on
14 other aspects of his professional and personal life. And shortly after the filing of his
15 complaint, the Defendant notified Ranson that it was going to perform an audit of his
16 billing and treatment, only to rescind that notification audit later that same day. Plaintiff
17 Ranson is informed and believes that the audit was prompted by his participation in this
18 lawsuit. He now monitors all his personal and business accounts for any sign of
19 tampering, theft, or identity fraud on a weekly basis.

20 9. Plaintiff Mitchell Flanders is a citizen and resident of Virginia. In 2018,
21 Plaintiff Flanders worked as an intern for Magellan Federal (formerly the Armed Forces
22 Services Corporation), another Magellan subsidiary, prior to being promoted to a full-
23 time position, where he worked until his resignation from the company in 2019. He is
24 currently unaffiliated with Magellan. Plaintiff Flanders received written notice of the
25 Data Breach, and a true and correct copy of that notice is attached hereto as Exhibit G.

26
27
28

¹ As an MHSA, Magellan manages healthcare services for approximately 40 million members nationwide, which includes the offering of provider networks.

1 Plaintiff Flanders has increased the time spent monitoring his accounts, and recently
2 learned that his data is being offered for sale on the “Dark Web,” as a result of the breach.

3 10. Plaintiff Joseph Rivera is a citizen and resident of Wisconsin. Plaintiff
4 Rivera was employed by Abbott Laboratories from May 2001 through May 2012. In
5 2012, Abbott Laboratories split into two divisions, and Plaintiff Rivera became an
6 employee of Abvie and continues to be employed with Abvie. During the time that
7 Plaintiff Rivera was employed by Abbot Laboratories (May 2001-May 2012), Magellan
8 Health administered Abbott Laboratories’ health care plan in which he was a participant.
9 Plaintiff Rivera received written notice of the Data Breach by letter dated June 18, 2020,
10 and a true and correct copy of that notice letter is attached hereto as Exhibit H.

11 11. Plaintiff Teresa Culberson is a citizen and resident of Tennessee. Plaintiff
12 Culberson was an insured under Magellan’s Rx Medicare program. On or about June 15,
13 2020, Plaintiff Culberson received a letter from Magellan notifying her that her
14 information was compromised as the result of an April 11, 2020 Data Breach at Magellan,
15 and a true and correct copy of that notice letter is attached hereto as Exhibit I.

16 12. Defendant Magellan Health is a publicly traded Delaware corporation
17 headquartered at 4801 E. Washington Street, Phoenix, Arizona 85034. It operates three
18 segments with various wholly owned subsidiaries, including but not limited to, HAIC
19 and Magellan Federal.

20 **JURISDICTION AND VENUE**

21 13. This Court has subject matter jurisdiction over this action under the Class
22 Action Fairness Act, 28 U.S.C. § 1332(d)(2). There are at least 100 putative Class
23 Members, the aggregated claims of the individual Class Members exceed the sum or
24 value of \$5,000,000 exclusive of interest and costs, and members of the proposed Class
25 are citizens of states different from Defendant.

26 14. This Court has jurisdiction over Defendant, which operates and is
27 headquartered in this District. The computer systems implicated in this Data Breach are
28 also likely based in this District. Through its business operations in this District, Magellan

1 and its related subsidiaries intentionally avail themselves of the markets within this
2 District to render the exercise of jurisdiction by this Court just and proper.

3 15. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a
4 substantial part of the events and omissions giving rise to this action occurred in this
5 District. Defendant is headquartered in this District, where it maintains personally
6 identifiable information (“PII”), and protected health information (“PHI”) on its current
7 and former employees as well as members participating in various health plans it
8 administers, and has caused harm to Plaintiffs and Class Members, some of whom reside
9 in this District.

10 NATURE OF THE ACTION

11 16. This class action arises out of the most recent targeted cyberattack and Data
12 Breach (“Data Breach”) involving Defendant and its subsidiaries and affiliates.² As a
13 result of the Data Breach, the PII and PHI of Plaintiffs and at least 365,000 Class
14 Members is in the hands of cyberthieves. Plaintiffs and Class Members suffered
15 ascertainable losses in the form of out-of-pocket expenses and the value of their time
16 reasonably incurred to remedy or mitigate the effects of the attack. In addition, Plaintiffs’
17 and Class Members’ sensitive personal information—which was entrusted to Magellan
18 Health, its officials and agents—was compromised and unlawfully accessed due to the
19 Data Breach. Information compromised in the Data Breach included names, contact
20 information, employee ID numbers, and W-2 or 1099 information, including Social
21 Security Numbers or taxpayer identification numbers, treatment information, health
22

23
24

² Magellan Health, Inc.’s affiliates involved in the breach include but are not limited to:
25 Magellan Healthcare, Inc. (55,637 patients), Merit Health Insurance Company (102,748
26 patients), Florida MHS, Inc. d/b/a Magellan Complete Care of Florida (76,236 patients),
27 the University of Florida Health Jacksonville (54,002 patients), MA Magellan GELLAN
28 Healthcare of Maryland, LLC (50,410 patients), VRx Pharmacy (33,040 patients),
National Imaging Associates, Inc. (22,560 patients), UF Health Shands (13,146 patients),
UF Health (9,182 patients), and Magellan Complete Care of Virginia, LLC (3,568
patients).

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

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

9 18. Defendant maintained the PII and PHI of its employees and health plan
10 participants in a reckless and negligent manner. In particular, the PII and PHI was
11 maintained on Defendant Magellan Health's computer network in a condition vulnerable
12 to cyberattacks. The mechanism of the cyberattack and potential for improper disclosure
13 of Plaintiffs' and Class Members' PII and PHI was a known risk to Defendant, as it was
14 subject to another Data Breach a mere 11 months prior that involved a similar phishing
15 attack. Thus Defendant was on notice that failing to take steps necessary to secure the PII
16 and PHI from those risks left that property in a dangerous condition.

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

20 20. Plaintiffs' and Class Members' identities are now at risk because of
21 Defendant's reckless and negligent conduct, because the PII and PHI that Defendant and
22 its affiliates collected and maintained is now in the hands of data thieves and available
23 on the dark web.

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

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

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

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

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

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

18 26. Accordingly, Plaintiffs bring this action against Defendant seeking redress
19 for its unlawful conduct, and asserting claims for: (i) negligence; (ii) negligence *per se*;
20 (iii) breach of implied contract; (iv) unjust enrichment; (v) violation of the Arizona
21 Consumer Fraud Act; (vi) violation of California's Unfair Competition Law; (vii)
22 violation of Missouri's Merchandising Practices Act; (viii) violation of New York's
23 General Business Law § 349; (ix) violation of Pennsylvania's Unfair and Deceptive
24 Trade Practices and Consumer Protection Law; (x) violation of Virginia's Personal
25 Information Breach Notification Act; and (xi) violation of Wisconsin's Deceptive Trade
26 Practices Act.

27 ///

28 //

1 **STATEMENT OF FACTS**

2 **A. *Defendant Magellan Health***

3 27. Incorporated in 1969 in Delaware, Defendant Magellan Health is a for-
4 profit managed health care company, focused on special populations, complete pharmacy
5 benefits and other specialty areas of healthcare.

6 28. It directly manages health benefits for its members' patients, including
7 those of its affiliates/subsidiaries Magellan Healthcare, Inc. (55,637 patients); Merit
8 Health Insurance Company (102,748 patients), Florida MHS, Inc. d/b/a Magellan
9 Complete Care of Florida (76,236 patients), the University of Florida Health Jacksonville
10 (54,002 patients), Magellan Healthcare of Maryland, LLC (50,410 patients), VRx
11 Pharmacy (33,040 patients), National Imaging Associates, Inc. (22,560 patients), UF
12 Health Shands (13,146 patients), UF Health (9,182 patients), and Magellan Complete
13 Care of Virginia, LLC (3,568 patients).

14 29. As part of its contractual relationship with the aforementioned
15 affiliates/subsidiaries and several other providers, Magellan administers the health and
16 pharmaceutical benefits offered by those affiliates/subsidiaries. Magellan Health
17 received fees from these affiliates or the states in which they operate to administer those
18 benefits and to provide services related to those benefits to Class Members, which
19 included storing the personal data of Class Members on its computers and computer
20 systems. The fees received by Defendant for these services are accrued and paid as a
21 result of Class Members' participation in and payment for these health and
22 pharmaceutical plans.

23 **B. *The Data Breach***

24 30. On or about April 6, 2020, an unauthorized person gained access to an
25 employee's e-mail by impersonating a client of Magellan. That access led to a
26 ransomware attack that allowed the person to gain access to and extract sensitive data
27 from a Magellan server.

28 //

1 31. The stolen data included sensitive PII and PHI, including names, addresses,
2 employees' ID numbers, and W-2 and 1099 details (including Social Security Numbers,
3 and Taxpayer ID numbers) of current and former employees and Magellan providers.

4 32. This was the second such Data Breach to occur at Magellan within the last
5 year, with notices of the breaches only surfacing within the last six months.

6 33. The first breach occurred on May 28, 2019, again after an unauthorized
7 third party had gained access to an employee email account through a commonplace
8 phishing attack. That breach resulted in the exposure of sensitive patient PHI and PII,
9 including patient names, Social Security Numbers, health plan member ID numbers,
10 health plan names, provider information, and prescription drug names.

11 34. However, despite discovering the breach during the summer, Magellan did
12 not notify individuals affected by the first breach until November of 2019. A related
13 class action concerning that breach has been filed in the Maricopa County Superior Court
14 of Arizona, Case No. CV2020-013648, after being previously filed in this District,
15 *Dearing v. Magellan Health, Inc., et al.*, 2:20-cv-0-0747-SPL (D. Ariz.).³

16 35. During the more recent breach, Magellan's servers were hit by a
17 ransomware attack. A ransomware attack deploys a type of malicious software that
18 blocks access to a computer system or data, usually by encrypting it, until the victim pays
19 a fee to the attacker.⁴

20 36. Magellan detected the ransomware attack on April 11, 2020 when files
21 were encrypted on its systems. An investigation into the attack allegedly revealed the
22 attacker had gained access to its systems following a response to a spear phishing email
23 sent on April 6.

24 ³ The first Magellan case was dismissed as to the 44,000 TennCare beneficiaries for
25 failure to allege Article III standing. The case was refiled in state court under the more
26 liberal state law standing requirements. The facts and the alleged injuries of the first
27 Magellan (TennCare) complaint are distinct from those presented here.

28 ⁴ *What Is Ransomware?* Proofpoint, <https://www.proofpoint.com/us/threat-reference/ransomware> (last visited October 28, 2020).

What We Are Doing

Magellan immediately reported the incident to, and is working closely with, the appropriate law enforcement authorities, including the FBI. Additionally, to help prevent a similar type of incident from occurring in the future, we implemented additional security protocols designed to protect out network, email environment, systems, and personal information.⁵

40. Upon information and belief, this notice was sent to 50,410 persons, and was reported to the U.S. Department of Health and Human Services ("HHS") on June 12, 2020.

41. On June 12, 2020, Defendant subsequently issued a second notice of Data Breach to the plan participants of Complete Care of Florida and Magellan Rx Pharmacy of Maryland and reported the Data Breach for Magellan Health to HHS. This notice was sent to 76,236 plan participants of Complete Care of Florida, and 33,040 plan participants of Magellan Rx Pharmacy of Maryland.

42. This second notice of Data Breach states, in pertinent part:

Notice of Security Incident

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

⁵ <https://oag.ca.gov/system/files/MAGELLAN%20-%20Sample%20Individual%20Notice.pdf> (last visited August 3, 2020). However, since the filing of the Second Amended Complaint in the *Griffey* matter, the page become unavailable. An archived version of the above URL can be found on the Internet Archive, available at <https://web.archive.org/web/20201005041745/https://oag.ca.gov/system/files/MAGELLAN%20-%20Sample%20Individual%20Notice.pdf> (last visited October 28, 2020).

1 *What Happened*

2 On April 11, 2020 we discovered that we were the target of a
3 ransomware attack. Immediately after discovering the incident
4 we retained a leading cybersecurity forensics firm, Mandiant,
5 to help conduct a thorough investigation of the incident. The
6 investigation revealed that the incident may have affected
7 personal information.

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

10 *What Information Was Involved*

11 The personal information included names and one or more of
12 the following: treatment information, health insurance account
13 information, member ID, other health-related information,
14 email addresses, phone numbers, and physical addresses. In
15 certain instances, Social Security Numbers were also affected.

16 *What Are We Doing*

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

23 A copy of this second notice is posted on Defendant's website.⁶

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

44. On June 15, 2020, Defendant issued a notice identical in form to the June
12, 2020 notice to persons affected by this Data Breach who were plan participants of

⁶ <https://www.magellanhealth.com/news/security-incident/> (last visited October 28, 2020).

1 Defendant's affiliate/subsidiary Magellan Complete Care of Virginia, LLC, and reported
2 the Data Breach for that affiliate to HHS on that same date.

3 45. On June 26, 2020, Defendant issued another notice of the Data Breach to
4 persons enrolled in health plans serviced by Defendant. This includes Plaintiff Leather.

5 46. The June 26, 2020 notice of Data Breach states, in pertinent part:

6 Magellan Health, Inc. ("Magellan") was recently the victim of
7 a criminal ransomware attack. We are writing to let you know how
8 this incident may have affected your personal information and, as a
9 precaution, to provide steps you can take to help protect your
10 information.

11 *What Happened*

12 On April 11, 2020, Magellan discovered it was targeted by a
13 ransomware attack. The unauthorized actor gained access to
14 Magellan's systems after sending a phishing email on April 6 that
15 impersonated a MAGE Magellan LLAN client. Once the incident was
16 discovered, Magellan immediately retained a leading cybersecurity
17 forensics firm, Mandiant, to help conduct a thorough investigation of
18 the incident. The investigation revealed that the incident may have
19 affected your personal information. At this point, we are not aware of
20 any fraud or misuse of any of your personal information as a result of
21 the incident, but are notifying you out of an abundance of caution.

22 *What Information Was Involved*

23 The personal information accessed by the unauthorized actor
24 included your Social Security number and/or other financial
25 information and possibly included names and one or more of the
26 following: treatment information, health insurance account
27 information, member ID, other health-related information, email
28 addresses, phone numbers, and physical addresses. In certain
instances, Social Security Numbers were also affected.

What Are We Doing

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

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

5 ***D. Magellan's Obligations to Keep PII and PHI Secure***

6 48. Due to its business and operations, Magellan is obligated by the Health
7 Insurance Portability and Accountability Act of 1996 ("HIPAA") to comply with a series
8 of administrative, physical security, and technical security requirements in order to
9 protect sensitive patient information. Among other things, the law mandates Magellan
10 develop, publish, and adhere to a privacy practice.

11 49. It is well known that healthcare organizations have been the target of an
12 increasing number of cyberattacks and, as a result, they must take adequate and
13 reasonable steps to protect their systems from attack, regardless of who the intended or
14 incidental victims are. This includes not only protecting patient information but also
15 employee data.

16 50. Defendant assures its patients, members and other consumers that "[y]our
17 personal privacy is important to us."⁷ Magellan Health's Privacy Policy further states:
18 "Magellan uses physical, technical, and administrative safeguards to protect any
19 personally identifiable data stored on its computers. Only authorized employees and third
20 parties have access to the information you provide to Magellan for providing service to
21 you."⁸

22 51. As such, Magellan recognizes its obligations under HIPAA to safeguard
23 and protect patient PHI and PII. These obligations also extend to Magellan employees,
24 as the company has an established Privacy Policy that details the types of PII and PHI

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

28 ⁸ *Id.*

1 Magellan collects from its employees, providers and patients, among others.⁹
2 Additionally, under various federal and state laws, regulations, industry practices and
3 common law, Magellan is bound to safeguard and protect the personal data of its
4 employees, providers, and patients to avoid unauthorized disclosure to third parties.

5 ***E. Prevalence of Cyber Attacks and Susceptibility of the Healthcare Sector***

6 52. Data Breaches have become widespread and especially so in healthcare. In
7 2016, the number of U.S. Data Breaches surpassed 1,000, a record high representing a
8 40% increase in the number of Data Breaches from the previous year. In 2017, another
9 record high of 1,579 breaches were reported, representing a 44.7% increase over 2016.¹⁰
10 In 2018, there was an extreme jump of 126% in the number of consumer records exposed
11 from Data Breaches. In 2019, there was a 17% increase in the number of breaches (1,473)
12 over 2018, with 164,683,455 sensitive records exposed.¹¹

13 53. Not surprisingly, companies in the business of storing and maintaining PII
14 and PHI, such as Magellan Health are among the most targeted—and therefore at risk—
15 for cyber-attacks.¹²

16 54. Cyberattacks may come in many forms. Phishing attacks are among the
17 oldest, most common, and well known. In simple terms, phishing is a method of

18
19 ⁹<https://www.magellanhealth.com/privacy-policy/#:~:text=MAGELLAN%20uses%20physical%2C%20technical%2C%20and,for%20providing%20service%20to%20you> (last visited October 28, 2020).

21 ¹⁰ Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review*,
22 <https://www.idtheftcenter.org/2017-data-breaches/> (last visited October 28, 2020).

23 ¹¹Identity Theft Resource Center *Identity Theft Resource Center's Annual End-of-Year*
24 *Data Breach Report Reveals 17 Percent Increase in Breaches Over 2018*,
25 <https://www.idtheftcenter.org/identity-theft-resource-centers-annual-end-of-year-data-breach-report-reveals-17-percent-increase-in-breaches-over-2018/> (last visited October
26 28, 2020).

27 ¹² Cyber Security Hub, *Top 8 Industries Reporting Data Breaches in The First Half Of*
28 *2019*, <https://www.cshub.com/attacks/articles/top-8-industries-reporting-data-breaches-in-the-first-half-of-2019> (last visited October 28, 2020).

1 obtaining personal information using deceptive e-mails and websites. The goal is to trick
2 an e-mail recipient into believing that the message is something they want or need from
3 a legitimate or trustworthy source and to subsequently take an action such as clicking on
4 a link or downloading an attachment. The fake link will typically mimic a familiar
5 website and require the input of credentials. Once input, the credentials are then used to
6 gain unauthorized access into a system. “It’s one of the oldest types of cyberattacks,
7 dating back to the 1990s” and one that every organization with an internet presence is
8 aware.”¹³ It remains the “simplest kind of cyberattack and, at the same time, the most
9 dangerous and effective.”¹⁴

10 55. Phishing attacks are well understood by the cyberprotection community
11 and are generally preventable with the implementation of a variety of proactive measures
12 such as sandboxing inbound e-mail¹⁵, inspecting and analyzing web traffic, penetration
13 testing¹⁶, and employee education, among others.

14
15 ¹³ *What is phishing? How this cyber attack works and how to prevent it*, CSO Online,
16 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 October 28, 2020).

17
18 ¹⁴ *Phishing*, Malwarebytes, <https://www.malwarebytes.com/phishing/> (last visited
October 28, 2020).

19
20 ¹⁵ Sandboxing is an automated process whereby e-mail with attachments and links are
21 segregated to an isolated test environment, or a “sandbox,” wherein a suspicious file or
URL may be executed safely.

22
23 ¹⁶ Penetration testing is the practice of testing a computer system, network, or web
24 application to find security vulnerabilities that an attacker could exploit. The main
25 objective of penetration testing is to identify security weaknesses. Penetration testing can
26 also be used to test an organization’s security policy, its adherence to compliance
27 requirements, its employees' security awareness and the organization's ability to identify
28 and respond to security incident. The primary goal of a penetration test is to identify weak
spots in an organization’s security posture, as well as measure the compliance of its
security policy, test the staff’s awareness of security issues and determine whether -- and
how -- the organization would be subject to security disasters. See
<https://searchsecurity.techtarget.com/definition/penetration-testing> (last visited October
28, 2020).

1 56. Among various data, healthcare related data is some of the most sensitive
2 and personally consequential when it is compromised. A report focusing on healthcare
3 breaches found that the “average total cost to resolve an identity theft-related
4 incident...came to about \$20,000,” and that the victims were often forced to pay out-of-
5 pocket costs for health care they did not receive in order to restore coverage.¹⁷ Almost
6 50% of the victims lost their health care coverage as a result of the incident, while nearly
7 one-third said their insurance premiums went up after the event. Forty percent of the
8 customers were never able to resolve their identity theft at all. Data Breaches and identity
9 theft have a crippling effect on individuals and detrimentally impact the economy.¹⁸

10 57. In recent years, the pace of breaches within healthcare organizations has
11 rapidly increased. According to a 2019 HIMSS Cybersecurity Survey, some 82% of
12 participating hospital information security leaders reported having a significant security
13 incident within the last 12 months, with a majority of these known incidents being caused
14 by “bad actors” such as cybercriminals.¹⁹ “Hospitals have emerged as a primary target
15 because they sit on a gold mine of sensitive personally identifiable information for
16 thousands of patients at any given time. From Social Security Numbers and insurance
17 policies to next of kin and credit cards, no other organization, including credit bureaus,
18 have so much monetizable information stored in their data centers.”²⁰

19 58. Indeed, the *HIPAA Journal* 2019 Healthcare Data Breach Report
20 demonstrates an upward trend in health sector Data Breaches over the past 10 years, with

21 ¹⁷ 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
23 visited October 28, 2020).

24 ¹⁸ *Id.*

25 ¹⁹ HIMSS, 2019 *HIMSS Cybersecurity Survey*, [https://www.himss.org/himss-](https://www.himss.org/himss-cybersecurity-survey)
26 [cybersecurity-survey](https://www.himss.org/himss-cybersecurity-survey) (last visited October 28, 2020).

27 ²⁰ Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*,
28 April 4, 2019, available at [https://www.idigitalhealth.com/news/how-to-safeguard-](https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks)
[hospital-data-from-email-spoofing-attacks](https://www.idigitalhealth.com/news/how-to-safeguard-hospital-data-from-email-spoofing-attacks) (last visited October 28, 2020).

1 2019 reflecting more Data Breaches than any other year.²¹ 2019 represented a 37.4%
2 increase over breaches reported in 2018 with a total number of patient records exposed
3 increasing from 13,947,909 in 2018 to 41,335,889.²² “Shockingly, the report disclosed
4 that in 2019 alone, the healthcare records of 12.55% of the population of the United States
5 were exposed, impermissibly disclosed, or stolen.”²³

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

12 ***F. Magellan Acquires, Collects, and Stores Plaintiffs’ and Class Members’ PII and***
13 ***PHI***

14 60. As its Privacy Policy makes clear, Magellan Health acquires, collects, and
15 stores a massive amount of PII on its employees, former employees, and beneficiaries.

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

19 62. Defendant also required Class Members to submit non-public personal
20 information, PII, and PHI in order to obtain medical and pharmacy services from its
21

22 ²¹ *Healthcare Data Breach Statistics*, HIPAA Journal, [https://www.hipaajournal.com/health](https://www.hipaajournal.com/health-care-data-breach-statistics/)
23 [care-data-breach-statistics/](https://www.hipaajournal.com/health-care-data-breach-statistics/) (last visited October 28, 2020).

24 ²² *2019 Healthcare Data Breach Report*, HIPAA Journal, <https://www.hipaajournal.com/2019-healthcare-data-breach-report/> (last visited October
25 28, 2020).
26

27 ²³ *Report Reveals Worst State for Healthcare Data Breaches in 2019*, Info Security
28 Group, February 14, 2020, [https://www.infosecurity-magazine.com/news/report-](https://www.infosecurity-magazine.com/news/report-healthcare-data-breaches-in/)
[healthcare-data-breaches-in/](https://www.infosecurity-magazine.com/news/report-healthcare-data-breaches-in/) (last visited October 28, 2020).

1 affiliates, and also creates PHI (e.g., treatment records) in the course of providing medical
2 and pharmacy services.

3 63. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and
4 Class Members' PII and PHI, Magellan assumed legal and equitable duties and knew or
5 should have known that it was responsible for protecting Plaintiffs' and Class Members'
6 PII and PHI from unauthorized disclosure.

7 64. At all times relevant hereto, Plaintiffs and Class Members took reasonable
8 steps to maintain the confidentiality of their PII and PHI. Plaintiffs and Class Members
9 relied on Magellan to keep their PII and PHI confidential and securely maintained, to use
10 this information for business purposes only, and to make only authorized disclosures of
11 this information.

12 ***G. The Value of Personally Identifiable Information and the Effects of***
13 ***Unauthorized Disclosure***

14 65. Personally identifiable information is a valuable commodity to identity
15 thieves. As the FTC recognizes, identity thieves can use it to commit an array of crimes
16 including identify theft, medical and financial fraud.²⁴ Indeed, a robust "cyber black
17 market" exists in which criminals openly post stolen PII on multiple underground Internet
18 websites.

19 66. While credit card information can sell for as little as \$1-\$2 on the black
20 market, other more sensitive information can sell for as much as \$363 according to the
21 Infosec Institute. PII is particularly valuable because criminals can use it to target victims
22 with frauds and scams. Once PII is stolen, fraudulent use of that information and damage
23 to victims may continue for years.

24 67. For example, the Social Security Administration has warned that identity
25 thieves can use an individual's Social Security Number to apply for additional credit

26
27 ²⁴ Federal Trade Commission, *Warning Signs of Identity Theft*,
28 <https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft> (last visited
October 28, 2020).

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

9 68. Moreover, it is not an easy task to change or cancel a stolen Social Security
10 Number. An individual cannot obtain a new Social Security Number without significant
11 paperwork and evidence of actual misuse. Even then, a new Social Security Number may
12 not be effective, as “[t]he credit bureaus and banks are able to link the new number very
13 quickly to the old number, so all of that old bad information is quickly inherited into the
14 new Social Security number.”²⁵

15 69. This data, as one would expect, demands a much higher price on the black
16 market. Martin Walter, senior director at cybersecurity firm RedSeal, explained,
17 “[c]ompared to credit card information, personally identifiable information and Social
18 Security Numbers are worth more than 10x on the black market.”²⁶ As explained above,
19 the inclusion of PHI, such as the information exposed here, is even more valuable.

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

23 ²⁵ *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Brian
24 Naylor, Feb. 9, 2015, <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft> (last visited October 28,
25 2020).

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

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

3 ***H. Magellan Failed to Comply with FTC Guidelines***

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

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

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

19 74. The FTC has brought enforcement actions against businesses for failing to
20 adequately and reasonably protect customer data, treating the failure to employ
21 reasonable and appropriate measures to protect against unauthorized access to
22 confidential consumer data as an unfair act or practice prohibited by Section 5 of the

23 ²⁷ Federal Trade Commission, *Start with Security*,
24 [https://www.ftc.gov/system/files/documents/plain-language/pdf0205-
25 startwithsecurity.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf) (last visited October 28, 2020).

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

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

1 Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these
2 actions further clarify the measures businesses must take to meet their data security
3 obligations.

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

8 76. Magellan was at all times fully aware of its obligation to protect the PII and
9 PHI of employees, providers and patients because of its position as an employer,
10 contractor and healthcare provider. Magellan was also aware of the significant
11 repercussions that would result from its failure to do so.

12 ***I. Magellan Failed to Comply with Industry Standards***

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

21 78. The Department of Health and Human Services’ Office for Civil Rights
22 (“HHS”) notes that “[w]hile all organizations need to implement policies, procedures,
23 and technical solutions to make it harder for hackers to gain access to their systems and
24 data, this is especially important in the healthcare industry. Hackers are actively targeting

25 _____
26 ³⁰ 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 (last visited October 28, 2020).

28 ³¹ *Id.*

1 healthcare organizations as they store large quantities of highly sensitive and valuable
2 data.”³² HHS highlights several basic cybersecurity safeguards that can be implemented
3 to improve cyber resilience which require a relatively small financial investment, yet can
4 have a major impact on an organization’s cybersecurity posture including: (a) the proper
5 encryption of PHI and PII; (b) educating and training healthcare employees on how to
6 protect PHI and PII; and (c) correcting the configuration of software and network devices.

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

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

18 ***J. Plaintiffs and Class Members Suffered Damages***

19 81. The ramifications of Defendant’s failure to keep employees’, patients’ and
20 providers’ PII and PHI secure are long lasting and severe. Once stolen, fraudulent use of
21
22
23

24 ³² *Cybersecurity Best Practices for Healthcare Organizations*, HIPAA Journal,
25 November 1, 2018, <https://www.hipaajournal.com/important-cybersecurity-best-practices-for-healthcare-organizations/> (last visited October 28, 2020).

27 ³³ *See, e.g.*, <https://resources.infosecinstitute.com/category/healthcare-information-security/is-best-practices-for-healthcare/10-best-practices-for-healthcare-security/#gref>
28 (last visited October 28, 2020).

1 such information and damage to victims may continue for years. Consumer victims of
2 Data Breaches are more likely to become victims of identity fraud.³⁴

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

7 83. Plaintiffs and Class Members have suffered actual injuries from having
8 their PII and PHI exposed as a result of the Data Breach, as identified elsewhere, and
9 including, but not limited to: (a) damages resulting from taking the time to search for
10 fraudulent activity; to change banks, bank accounts and debit and credit cards; to
11 purchase credit monitoring and identity theft protection; to call their creditors to provide
12 them with notice of the breach; and to otherwise attempt to protect their financial
13 accounts; (b) damages to and diminution in the value of their PII—a form of intangible
14 property that the Plaintiffs entrusted to Magellan as a condition of employment and the
15 provision of services to patients; (c) imminent and impending injury arising from the
16 increased risk of fraud and identity theft; and (d) in other ways to be discovered and
17 proven at trial.

18 84. As a result of the Data Breach, Plaintiffs and Class Members will continue
19 to be at heightened risk for financial fraud, medical fraud, identity theft, and attendant
20 damages for years, if not decades, to come.

21 85. The Data Breach was a direct and proximate result of Magellan's failure
22 to: (a) properly safeguard and protect Plaintiffs' and Class Members' PII and PHI from
23 unauthorized access, use, and disclosure, as required by various state and federal
24 regulations, industry practices, and common law; (b) establish and implement appropriate
25 administrative, technical, and physical safeguards to ensure the security and
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
October 28, 2020).

1 confidentiality of Plaintiffs' and Class Members' PII and PHI; (c) protect against
2 reasonably foreseeable threats to the security or integrity of such information; and (d) in
3 other ways to be discovered and proven at trial.

4 86. Defendant had the resources necessary to prevent the Data Breach, but
5 neglected to adequately invest in data security measures, despite its obligations to protect
6 PII and PHI. Had Defendant remedied the deficiencies in its data security systems and
7 adopted security measures recommended by experts in the field, especially given the
8 previous breach, it would have certainly prevented the intrusions into its systems and,
9 ultimately, the theft of PII and PHI here.

10 87. As a direct and proximate result of Defendant's wrongful actions and
11 inactions, Plaintiffs and Class Members have been placed at an imminent, immediate,
12 and continuing increased risk of harm from identity theft and fraud, requiring them to
13 take time away from other life demands such as work and family to mitigate the actual
14 and potential impact of the Data Breach on their lives. The U.S. Department of Justice's
15 Bureau of Justice Statistics found that "among victims who had personal information
16 used for fraudulent purposes, 29% spent a month or more resolving problems" and that
17 "resolving the problems caused by identity theft [could] take more than a year for some
18 victims."³⁵

19 88. To date, Magellan has offered inadequate identity monitoring services to
20 affected individuals given the type of data stolen. They are wholly inadequate as they
21 fail to provide for the fact that victims of Data Breaches and other unauthorized
22 disclosures commonly face multiple years of ongoing identity theft and financial fraud
23 and they entirely fail to provide any compensation for the unauthorized release and
24 disclosure of Plaintiffs' and Class Members' PII and PHI.

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*
<https://www.bjs.gov/content/pub/pdf/vit12.pdf> (last visited October 28, 2020).

1 89. As a result of the Defendant’s failures to prevent the Data Breach, Plaintiffs
2 and Class Members have suffered, will suffer, or are at increased risk of suffering:

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

21 90. In addition to a remedy for the economic harm, Plaintiffs and Class
22 Members maintain an undeniable interest in ensuring that their PII and PHI are secure,
23 remain secure, and are not subject to further misappropriation and theft.

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

27 92. The United States Government Accountability Office released a report in
28 2007 regarding Data Breaches (“GOA Report”) in which it noted that victims of identity

1 theft will face “substantial costs and time to repair the damage to their good name and
2 credit record.”³⁶

3 93. The FTC recommends that identity theft victims take several steps to
4 protect their personal and financial information after a Data Breach, including contacting
5 one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts
6 for 7 years if someone steals their identity), reviewing their credit reports, contacting
7 companies to remove fraudulent charges from their accounts, placing a credit freeze on
8 their credit, and correcting their credit reports.³⁷

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

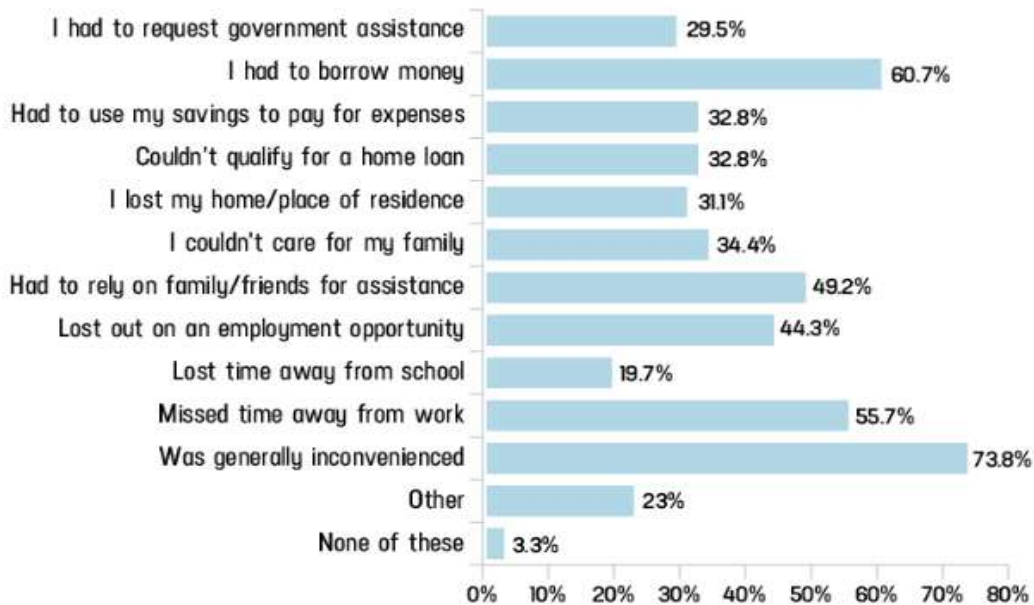
12 95. Identity thieves can also use Social Security Numbers to obtain a driver’s
13 license or official identification card in the victim’s name but with the thief’s picture; use
14 the victim’s name and Social Security number to obtain government benefits; or file a
15 fraudulent tax return using the victim’s information. In addition, identity thieves may
16 obtain a job using the victim’s Social Security number, rent a house or receive medical
17 services in the victim’s name, and may even give the victim’s personal information to
18 police during an arrest resulting in an arrest warrant being issued in the victim’s name. A
19 study by Identity Theft Resource Center shows the multitude of harms caused by
20 fraudulent use of personal and financial information:³⁸

21
22
23 ³⁶ See “*Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*,” U.S. Government Accountability Office, June
24 2007, *2, <https://www.gao.gov/new.items/d07737.pdf> (last visited October 28, 2020)
25 (“GAO Report”).

26 ³⁷ See <https://www.identitytheft.gov/Steps> (last visited October 28, 2020).

27 ³⁸ Jason Steele, *Credit Card and ID Theft Statistics*, October 24, 2017,
28 [https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-
statistics-1276.php](https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php) (last visited last visited October 28, 2020).

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



Source: Identity Theft Resource Center

creditcards.com

96. What's more, PII constitutes a valuable property right, the theft of which is gravely serious.³⁹ Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

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

[L]aw enforcement officials told us that in some cases, stolen data

³⁹ See, e.g., John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets") (citations omitted).

1 may be held for up to a year or more before being used to commit
2 identity theft. Further, once stolen data have been sold or posted on
3 the Web, fraudulent use of that information may continue for years.
As a result, studies that attempt to measure the harm resulting from
Data Breaches cannot necessarily rule out all future harm.

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

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

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

13 **CLASS ACTION ALLEGATIONS**

14 100. Plaintiffs seek relief on behalf of themselves and as representatives of all
15 others who are similarly situated. Pursuant to Fed. R. Civ. P. Rule 23(a), (b)(2), (b)(3)
16 and (c)(4), Plaintiffs seek certification of a Nationwide class defined as follows:

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

19 101. Alternatively, Plaintiffs propose the following definitions for the following
20 subclasses of Class Members (collectively, “Subclasses”);

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

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

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

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

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

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

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

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

12 102. Excluded from the Class are Magellan and any of its affiliates, parents or
13 subsidiaries; all persons who make a timely election to be excluded from the Class;
14 government entities; and the judges to whom this case is assigned, their immediate
15 families, and court staff.

16 103. Plaintiffs hereby reserve the right to amend or modify the Class definition
17 with greater specificity or division after having had an opportunity to conduct discovery.

18 104. The proposed Class meets the criteria for certification under Rule 23(a),
19 (b)(2), (b)(3), and (c)(4).

20 105. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the
21 members of the Class are so numerous that the joinder of all members is impractical.
22 The Data Breach implicates approximately 10,500 Magellan employees, both current
23 and former, as well as a potentially unknown number of Magellan providers and other
24 health plan participants.

25 106. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Rule
26 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common
27
28

1 questions of law and fact that predominate over any questions affecting individual Class
2 Members. The common questions include:

- 3 a. Whether Magellan had a duty to protect its employees', providers'
4 and patients' sensitive PII and PHI;
- 5 b. Whether Magellan knew or should have known of the susceptibility
6 of its systems to a Data Breach;
- 7 c. Whether Magellan's security measures to protect its systems were
8 reasonable in light of best practices recommended by data security
9 experts;
- 10 d. Whether Magellan was negligent in failing to implement reasonable
11 and adequate security procedures and practices;
- 12 e. Whether Magellan's failure to implement adequate data security
13 measures allowed the breach of its data systems to occur;
- 14 f. Whether Magellan's conduct, including its failure to act, resulted in
15 or was the proximate cause of the breach of its systems, resulting in
16 the unlawful exposure of the Plaintiffs' and Class Members' PII and
17 PHI;
- 18 g. Whether Plaintiffs and Class Members were injured and suffered
19 damages or other losses because of Magellan's failure to reasonably
20 protect its systems and data network; and,
- 21 h. Whether Plaintiffs and Class Members are entitled to relief.

22 **107. Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Rule 23(a)(3),
23 Plaintiffs' claims are typical of those of other Class Members. Plaintiffs were former
24 and current employees of various Magellan entities, providers and other persons
25 believed to work on a 1099 basis with a Magellan entity – all of whom had their PII
26 exposed in the Data Breach and members of various health plans serviced by Magellan.
27 Plaintiffs' damages and injuries are akin to other Class Members, and Plaintiffs seek
28 relief consistent with the relief sought by the Class.

1 **108. Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4),
2 Plaintiffs are adequate representatives of the Class because they are members of the
3 Class they seek to represent; are committed to pursuing this matter against Magellan to
4 obtain relief for the Class; and have no conflicts of interest with the Class. Moreover,
5 Plaintiffs' attorneys are competent and experienced in litigating class actions, including
6 privacy litigation of this kind. Plaintiffs intend to vigorously prosecute this case and will
7 fairly and adequately protect the Class' interests.

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

23 **110. Injunctive and Declaratory Relief.** Class certification is also appropriate
24 under Rule 23(b)(2) and (c). Defendant, through its uniform conduct, acted or refused to
25 act on grounds generally applicable to the Class as a whole, making injunctive and
26 declaratory relief appropriate to the Class as a whole.

27 **111.** Likewise, particular issues under Rule 23(c)(4) are appropriate for
28 certification because such claims present only particular, common issues, the resolution

1 of which would advance the disposition of this matter and the parties' interests therein.

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

- 3 a. Whether Magellan owed a legal duty to Plaintiffs and the Class to
4 exercise due care in collecting, storing, and safeguarding their PII
5 and PHI;
- 6 b. Whether Magellan's security measures to protect its data systems
7 were reasonable in light of best practices recommended by data
8 security experts;
- 9 c. Whether Magellan's failure to institute adequate protective security
10 measures amounted to negligence;
- 11 d. Whether Magellan failed to take commercially reasonable steps to
12 safeguard employee, provider and patient PII and PHI;
- 13 e. Whether adherence to FTC data security recommendations, and
14 measures recommended by data security experts would have
15 reasonably prevented the Data Breach; and
- 16 f. Whether Magellan failed to comply with its statutory and regulatory
17 obligations.

18 112. Finally, all members of the proposed Class are readily ascertainable.
19 Magellan has access to its employees', providers' and patients' names and addresses
20 affected by the Data Breach. Using this information, Class Members can be identified
21 and ascertained for the purpose of providing notice.

22 **FIRST CAUSE OF ACTION**
23 **NEGLIGENCE**

24 *(On Behalf of all Plaintiffs, the Nationwide Class, and all Subclasses)*

25 113. Plaintiffs restate and reallege paragraphs 1 through 112 as if fully set forth
26 herein.

27 ///

28 //

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

4 115. Plaintiffs and all Class Members entrusted their PII and PHI to Magellan
5 Health with the understanding that the Defendant would safeguard their information.

6 116. Magellan Health had full knowledge of the sensitivity of this PII and PHI
7 and the types of harm that Plaintiffs and Class Members could and would suffer if such
8 information was wrongfully disclosed.

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

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

21 119. Defendant’s duty to use reasonable security measures under HIPAA
22 required Defendant to “reasonably protect” confidential data from “any intentional or
23 unintentional use or disclosure” and to “have in place appropriate administrative,
24 technical, and physical safeguards to protect the privacy of protected health information.”
25 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case
26 constitutes “protected health information” within the meaning of HIPAA.

27 ///

28 //

1 120. Defendant’s duty to use reasonable care in protecting confidential data
2 arose not only as a result of the statutes and regulations described above, but also because
3 Defendant is bound by industry standards to protect confidential PII and PHI.

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

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

19 122. It was foreseeable that Defendant’s failure to use reasonable measures to
20 protect Class Members’ PII and PHI would result in injury to Class Members. Further,
21 the breach of security was reasonably foreseeable given the known high frequency of
22 cyberattacks and Data Breaches in the data storage and healthcare industries.

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

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

28 //

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

3 126. Defendant was able to protect against the harm suffered by Plaintiffs and
4 Class Members as a result of the Data Breach.

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

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

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

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

18 131. Plaintiffs and Class Members are also entitled to injunctive relief requiring
19 Defendant to, *e.g.*, (a) strengthen their data security systems and monitoring procedures;
20 (b) submit to future annual audits of those systems and monitoring procedures; and (c)
21 continue to provide adequate credit monitoring to all Class Members.

22 **SECOND CAUSE OF ACTION**
23 **NEGLIGENCE *PER SE***

24 *(On Behalf of all Plaintiffs, the Nationwide Class, and all Subclasses)*

25 132. Plaintiffs restate and reallege paragraphs 1 through 112 as if fully set forth
26 herein.

27 ///

28 //

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

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

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

15 136. Defendant’s violation of Section 5 of the FTC Act constitutes negligence
16 *per se* as Defendant’s violation of the FTC Act establishes the duty and breach elements
17 of negligence.

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

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

25 139. Pursuant to the Gramm-Leach-Bliley Act (15 U.S.C. § 6801), Defendant
26 had a duty to protect the security and confidentiality of Plaintiffs’ and Class Members’
27 PII.

28 //

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

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

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

12 143. Defendant's failure to comply with applicable laws and regulations
13 constitutes negligence *per se*.

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

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

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

24 147. Plaintiffs and Class Members are also entitled to injunctive relief requiring
25 Defendant to, *e.g.*, (a) strengthen its data security systems and monitoring procedures;
26 (b) submit to future annual audits of those systems and monitoring procedures; and (c)
27 continue to provide adequate credit monitoring to all Class Members.

28 //

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT

(On Behalf of all Plaintiffs, the Nationwide Class, and all Subclasses)

148. Plaintiffs restate and reallege paragraphs 1 through 112 as if fully set forth herein.

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

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

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

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

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

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

//

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

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

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

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

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

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

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

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

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

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

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

5 *(On Behalf of all Plaintiffs, the Nationwide Class, and all Subclasses)*

6 164. Plaintiffs restate and reallege paragraphs 1 through 112 as if fully set forth
7 herein.

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

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

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

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

26 169. Plaintiffs and Class Members have no adequate remedy at law.

27 170. As a direct and proximate result of Defendant's conduct, Plaintiffs and
28 Class Members have suffered and will suffer injury, including but not limited to: (a)

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

14 171. As a direct and proximate result of Defendant’s conduct, Plaintiffs and
15 Class Members have suffered and will continue to suffer other forms of injury and/or
16 harm.

17 172. Defendant should be compelled to disgorge into a common fund or
18 constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that it
19 unjustly received from them.

20 173. Plaintiffs and Class Members are also entitled to injunctive relief requiring
21 Defendant to, *e.g.*, (a) strengthen its data security systems and monitoring procedures;
22 (b) submit to future annual audits of those systems and monitoring procedures; and (c)
23 continue to provide adequate credit monitoring to all Class Members.

24 ///

25 ///

26 ///

27 ///

28 //

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

(On Behalf of all Plaintiffs, the Nationwide Class, and the Arizona Subclass)

174. Plaintiffs restate and reallege paragraphs 1 through 112 as if fully set forth herein.

175. 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.

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

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

178. 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 Plaintiffs’ and Class Members’ confidential 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 maintaining adequate data privacy and security practices and procedures to safeguard Class Members' PII and PHI from unauthorized disclosure, release, Data Breaches, and theft;
- d. Misrepresenting material facts, in connection with the sale of health benefit services by representing that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Class Members' PHI and PII;
- e. Omitting, suppressing, and concealing the material fact of the inadequacy of the data privacy and security protections for Class Members' PHI and PII;
- f. Engaging in unfair, unlawful, and deceptive acts and practices with respect to the sale of health benefit services by failing to maintain the privacy and security of Class Members' PHI and PII, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair, unlawful, and deceptive acts and practices violated duties imposed by laws, including HIPAA and Section 5 of the FTC Act;
- g. Engaging in unlawful, unfair, and deceptive acts and practices with respect to the sale of health benefit services by failing to disclose the Data Breach to Class Members in a timely and accurate manner; and
- 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.

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

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

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

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

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

15 183. Plaintiffs and Class Members are also entitled to injunctive relief requiring
16 Defendant to, *e.g.*, (a) strengthen its data security systems and monitoring procedures;
17 (b) submit to future annual audits of those systems and monitoring procedures; and (c)
18 continue to provide adequate credit monitoring to all Class Members.

19 **SIXTH CAUSE OF ACTION**
20 **VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW**
21 **Cal. Bus. & Prof. Code §§ 17200, *et seq.***

22 *(On Behalf of Plaintiff Ranson and the California Subclass)*

23 184. Plaintiffs restate and reallege paragraphs 1 through 112 as if fully set forth
24 herein.

25 185. Magellan Health is a "person" as defined by Cal. Bus. & Prof. Code §
26 17201.

27 186. Magellan Health violated Cal. Bus. & Prof. Code §§ 17200, *et seq.*
28 ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

1 187. Magellan Health’s unlawful, unfair acts and deceptive acts and practices
2 include:

- 3 a. Magellan Health failed to implement and maintain reasonable
4 security measures to protect Plaintiff’s and California Class
5 Members’ PII and PHI from unauthorized disclosure, release, Data
6 Breaches, and theft, which was a direct and proximate cause of the
7 Data Breach;
- 8 b. Magellan Health failed to identify foreseeable security risks,
9 remediate identified security risks, and adequately improve security
10 following at least one previous cybersecurity incident within the last
11 year. This conduct, with little if any utility, is unfair when weighed
12 against the harm to Plaintiff and California Class Members whose
13 PII and PHI has been compromised;
- 14 c. Magellan Health’s failure to implement and maintain reasonable
15 security measures also was contrary to legislatively declared public
16 policy that seeks to protect consumer data and ensure that entities
17 that are trusted with it use appropriate security measures. These
18 policies are reflected in laws, including the FTC Act, 15 U.S.C. §
19 45, California’s Consumer Records Act, Cal. Civ. Code §§
20 1798.81.5 *et seq.*, and California’s Consumer Privacy Act, Cal. Civ.
21 Code §§ 1798.100 *et seq.*;
- 22 d. Magellan Health’s failure to implement and maintain reasonable
23 security measures also lead to substantial injuries, as described
24 above, that are not outweighed by any countervailing benefits to
25 consumers or competition. Moreover, because Plaintiff and
26 California Class Members could not know of Magellan Health’s
27 inadequate security, consumers could not have reasonably avoided
28 the harms that Magellan Health caused;

- 1 e. Misrepresenting that it would protect the privacy and confidentiality
- 2 of Plaintiff's and the California Class Members' PII, including by
- 3 implementing and maintaining reasonable security measures;
- 4 f. Misrepresenting that it would comply with common law and
- 5 statutory duties pertaining to the security and privacy of Plaintiff's
- 6 and the California Class Members' PII, including duties imposed by
- 7 the FTC Act, 15 U.S.C § 45; California's Customer Records Act,
- 8 Cal. Civ. Code §§ 1798.80, *et seq.*; and California's Consumer
- 9 Privacy Act, Cal. Civ. Code §§ 1798.100 *et seq.*;
- 10 g. Omitting, suppressing, and concealing the material fact that it did
- 11 not reasonably or adequately secure Plaintiff's and the California
- 12 Class Members' PII;
- 13 h. Omitting, suppressing, and concealing the material fact that it did
- 14 not comply with common law and statutory duties pertaining to the
- 15 security and privacy of Plaintiff's and the California Class
- 16 Members' PII, including duties imposed by the FTC Act, 15 U.S.C
- 17 § 45; California's Customer Records Act, Cal. Civ. Code §§
- 18 1798.80, *et seq.*; and California's Consumer Privacy Act, Cal. Civ.
- 19 Code §§ 1798.100 *et seq.*;
- 20 i. Engaging in unlawful business practices by violating Cal. Civ. Code
- 21 § 1798.82; and
- 22 j. Among other ways to be discovered and proved at trial.

23 188. Magellan Health representations and omissions to Plaintiff and California
24 Class Members were material because they were likely to deceive reasonable consumers
25 about the adequacy of Magellan Health's data security and ability to protect the
26 confidentiality of consumers' PII and PHI.

27 189. Magellan Health intended to mislead Plaintiff and the California Class
28 Members and induce them to rely on its misrepresentations and omissions.

1 190. Had Magellan Health disclosed to Plaintiff and the California Class
2 Members that its data systems were not secure and, thus, vulnerable to attack, Magellan
3 Health would have been unable to continue in business and it would have been forced to
4 adopt reasonable data security measures and comply with the law. Instead, Magellan
5 Health received, maintained, and compiled Plaintiff's and the California Class Members'
6 PII and PHI as part of the services and goods Magellan Health provided without advising
7 Plaintiff and the California Class Members that Magellan Health's data security practices
8 were insufficient to maintain the safety and confidentiality of Plaintiff's and the
9 California Class Members' PII and PHI. Accordingly, Plaintiff and the California Class
10 Members acted reasonably in relying on Magellan Health's misrepresentations and
11 omissions, the truth of which they could not have discovered.

12 191. Magellan Health acted intentionally, knowingly, and maliciously to violate
13 California's Unfair Competition Law, and recklessly disregarded Plaintiff's and the
14 California Class Members' rights, especially given that a similar attack had occurred
15 some 11 months previously.

16 192. As a direct and proximate result of Magellan Health's unfair, unlawful, and
17 fraudulent acts and practices, Plaintiff and California Class Members have suffered and
18 will continue to suffer injury, ascertainable losses of money or property, and monetary
19 and non-monetary damages as described herein and as will be proved at trial. These losses
20 include the diminished value of Plaintiff's and California Class Members' PII and PHI.
21 Because the integrity of Plaintiff's and California Class Members' PII is crucial to their
22 future ability to engage in many aspects of commerce, including obtaining a mortgage,
23 credit card, business loan, tax return, or even applying for a job, the diminishment of the
24 integrity of that PII and PHI corresponds to a diminishment in value. In other words,
25 Plaintiff and California Class Members have both present and future property interest
26 diminished as a result of Magellan Health's unfair, unlawful, and fraudulent acts and
27 practices.

28 //

1 193. Plaintiff and California Class Members seek all monetary and non-
2 monetary relief allowed by law, including restitution of all profits stemming from
3 Magellan Health’s unfair, unlawful, and fraudulent business practices or use of their PII;
4 declaratory relief; injunctive relief; reasonable attorneys’ fees and costs under California
5 Code of Civil Procedure § 1021.5; and other appropriate equitable relief.

6 194. Plaintiff and California Class Members are also entitled to injunctive relief
7 requiring Defendant to, *e.g.*, (a) strengthen its data security systems and monitoring
8 procedures; (b) submit to future annual audits of those systems and monitoring
9 procedures; and (c) continue to provide adequate credit monitoring to all California Class
10 Members.

11
12 **SEVENTH CAUSE OF ACTION**
13 **VIOLATION OF MISSOURI MERCHANDISING PRACTICES ACT**
14 **(“MMPA”)**
15 **MO. REV. STAT. § 407.010, *et seq.***

16 *(On Behalf of Plaintiff Griffey and the Missouri Subclass)*

17 195. Plaintiffs restate and reallege paragraphs 1 through 112 as if fully set forth
18 herein.

19 196. Magellan Health, Plaintiff and the Missouri Class are “persons” within the
20 meaning of Mo. Rev. Stat. § 407.010(5).

21 197. Healthcare services are a good.

22 198. Efforts to maintain the privacy and confidentiality of medical records are
23 part of the healthcare services associated with a good.

24 199. Maintenance of medical records are “merchandise” within the meaning of
25 section 407.010(4).

26 200. As set forth herein, Defendant’s acts, practices and conduct violate section
27 407.020(1) in that, among other things, Defendant has used and/or continues to use unfair
28 practices, concealment, suppression and/or omission of material facts in connection with

1 the advertising, marketing, and offering for sale of services associated with healthcare
2 services.

3 201. Defendant's unfair, unlawful and deceptive acts, practices, and conduct
4 include: (a) representing to its patients that it will not disclose their sensitive personal
5 health information to an unauthorized third party or parties; (b) failing to implement
6 security measures such as securing the records in a safe place; and (c) failing to train
7 personnel. Defendant's conduct violates the MMPA.

8 202. Defendant's conduct also violates the enabling regulations for the MMPA
9 because it: (a) offends public policy; (b) is unethical, oppressive, and unscrupulous; (c)
10 causes substantial injury to consumers; (d) is not in good faith; (e) is unconscionable; and
11 (f) is unlawful. See Mo. Code Regs. Ann. tit. 15, § 60-8.

12 203. As a direct and proximate result of Defendant's unfair and deceptive acts,
13 Plaintiff and Missouri Class Members have suffered damages in that they (a) paid more
14 for medical record privacy protections than they otherwise would have, and (b) paid for
15 medical record privacy protections that they did not receive. In this respect, Plaintiff and
16 Missouri Class Members have not received the benefit of their bargain, and have suffered
17 an ascertainable loss.

18 204. As such, Plaintiff and Missouri Class Members are entitled to seek actual
19 damages from Defendant; a declaration that Defendant's methods, acts and practices
20 violate the Missouri Merchandising Practices Act, Mo. Rev. Stat. §§ 407.010, *et seq.*, an
21 injunction prohibiting Defendant from continuing to engage in such unlawful methods,
22 acts, and practices; restitution; rescission; disgorgement of all profits obtained from
23 Defendant's unlawful conduct; pre and post-judgment interest; attorneys' fees and costs;
24 and any other relief that the Court deems necessary or proper.

25 205. Plaintiff and Missouri Class Members are also entitled to injunctive relief
26 requiring Defendant to, *e.g.*, (a) strengthen its data security systems and monitoring
27 procedures; (b) submit to future annual audits of those systems and monitoring
28

1 procedures; and (c) continue to provide adequate credit monitoring to all Missouri Class
2 Members.

3 **EIGHTH CAUSE OF ACTION**
4 **VIOLATION OF NEW YORK**
5 **GENERAL BUSINESS LAW § 349**

6 *(On Behalf of Plaintiff Leather and the New York Subclass)*

7 206. Plaintiffs restate and reallege paragraphs 1 through 112 as if fully set forth
8 herein.

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

- 12 a. Defendant misrepresented material facts to Plaintiff and the Class
13 by representing that it would maintain adequate data privacy and
14 security practices and procedures to safeguard Plaintiff and New
15 York Class Members' PHI and PII from unauthorized disclosure,
16 release, Data Breaches, and theft;
- 17 b. Defendant misrepresented material facts to Plaintiff and the New
18 York Subclass by representing that it did and would comply with
19 the requirements of federal and state laws pertaining to the privacy
20 and security of New York Class Members' PHI and PII;
- 21 c. Defendant omitted, suppressed and concealed material facts of the
22 inadequacy of its privacy and security protections for Plaintiff's and
23 New York Class Members' PHI and PII;
- 24 d. Defendant engaged in deceptive, unfair, and unlawful trade acts or
25 practices by failing to maintain the privacy and security of Plaintiff's
26 New York Class Members' PHI and PII, in violation of duties
27 imposed by and public policies reflected in applicable federal and
28

1 state laws, resulting in the Data Breach. These unfair acts and
2 practices violated duties imposed by laws including the Federal
3 Trade Commission Act (15 U.S.C. § 45); and

4 e. Defendant engaged in deceptive, unfair, and unlawful trade acts or
5 practices by failing to disclose the Data Breach to Plaintiff and the
6 Class in a timely and accurate manner, contrary to the duties
7 imposed by N.Y. Gen. Bus. Law § 899-aa(2). At all times relevant
8 herein, Plaintiff Leather and members of the New York Class were
9 residents of the State of New York and were deceived in New York
10 by the misconduct alleged herein.

11 208. Defendant knew or should have known that its computer systems and data
12 security practices were inadequate to safeguard Plaintiff's and the New York Class
13 Members' PHI and PII entrusted to it, and that risk of a Data Breach or theft was highly
14 likely.

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

17 210. Defendant's failure constitutes false and misleading representations, which
18 have the capacity, tendency, and effect of deceiving or misleading consumers (including
19 Plaintiff and New York Class Members) regarding the security of Magellan Health's
20 network and aggregation of PHI and PII.

21 211. The representations upon which consumers (including Plaintiff and New
22 York Class Members) relied were material representations (*e.g.*, as to Defendant's
23 adequate protection of PHI and PII), and consumers (including Plaintiff and New York
24 Class Members) relied on those representations to their detriment.

25 212. Defendant's conduct is unconscionable, deceptive, and unfair, as it is likely
26 to, and did, mislead consumers acting reasonably under the circumstances. As a direct
27 and proximate result of Defendant's conduct, Plaintiff and other New York Class
28 Members have been harmed, in that they were not timely notified of the Data Breach,

1 which resulted in profound vulnerability to their personal information and other financial
2 accounts.

3 213. As a direct and proximate result of Defendant’s unconscionable, unfair, and
4 deceptive acts and omissions, Plaintiff’s and New York Class Members’ PHI and PII was
5 disclosed to third parties without authorization, causing and will continue to cause
6 Plaintiff and Class Members damages, as well as to the public interest and consumers at
7 large in New York.

8 214. Plaintiff and New York Class Members seek relief under N.Y. Gen. Bus.
9 Law § 349(h), including, but not limited to, actual damages, treble damages, statutory
10 damages, injunctive relief, and/or attorney’s fees and costs.

11 215. Plaintiff and New York Class Members are also entitled to injunctive relief
12 requiring Defendant to, *e.g.*, (a) strengthen its data security systems and monitoring
13 procedures; (b) submit to future annual audits of those systems and monitoring
14 procedures; and (c) continue to provide adequate credit monitoring to all New York Class
15 Members.

16 **NINTH CAUSE OF ACTION**
17 **VIOLATION OF PENNSYLVANIA UNFAIR TRADE PRACTICES AND**
18 **CONSUMER PROTECTION LAW (73 P.S. § 201-1, *et seq.*)**

19 *(On Behalf of Plaintiff Domingo and the Pennsylvania Subclass)*

20 216. Plaintiff restates and realleges paragraphs 1 through 112 as if fully set forth
21 herein.

22 217. Plaintiff and Defendant are “persons” as defined at 73 Pa. Stat. § 201-2(2).

23 218. Plaintiff and Pennsylvania Class Members purchased goods and services in
24 “trade” and “commerce” as defined at 73 Pa. Stat. § 201-2(3).

25 219. Plaintiff and Pennsylvania Class Members purchased goods and services
26 primarily for personal, family, and/or household purposes under 73 Pa. Stat. § 201-9.2.

27 ///

28 //

1 220. Magellan Health engaged in “unfair methods of competition” or “unfair or
2 deceptive acts or practices” as defined at 73 Pa. Stat. § 201-2(4) by, among other things,
3 engaging in the following conduct:

- 4 a. Representing that its goods and services had characteristics, uses, benefits,
5 and qualities that they did not have – namely that its goods, services, and
6 business practices were accompanied by adequate data security (73 Pa.
7 Stat. § 201-2(4)(v));
- 8 b. Representing that its goods and services were of a particular standard or
9 quality when they were of another standard or quality (73 Pa. Stat. § 201-
10 2(4)(vii));
- 11 c. Advertising its goods and services with intent not to sell them as advertised
12 (73 Pa. Stat. § 201-2(4)(ix); and
- 13 d. “Engaging in any other ... deceptive conduct which creates a likelihood of
14 confusion or of misunderstanding” (73 Pa. Stat. § 201-2(4)(xxi)).

15 221. These unfair methods of competition and unfair or deceptive acts or
16 practices are declared unlawful by 73 Pa. Stat. § 201-3.

17 222. Magellan Health’s unfair or deceptive acts and practices include but are not
18 limited to: failing to implement and maintain reasonable data security measures to protect
19 Plaintiff’s and Pennsylvania Class Members’ PII and PHI; failing to identify foreseeable
20 data security risks and remediate the identified risks; failing to comply with common law
21 duties, industry standards including FTC guidance regarding data security;
22 misrepresenting in its Privacy Policy that it would protect Plaintiff’s and Pennsylvania
23 Class Members’ PII and PHI from unauthorized disclosure; and omitting and concealing
24 the material fact that it did not have reasonable measures in place to safeguard such data
25 from thieves stealing it.

26 223. Magellan Health’s representations and omissions were material because
27 they were likely to deceive reasonable consumers including Plaintiff and Pennsylvania
28

1 Class Members about the adequacy of Magellan Health’s data security practices and
2 ability to protect their PII and PHI.

3 224. Magellan Health intended to mislead Plaintiff and Pennsylvania Class
4 Members and induce them to rely on its misrepresentations and omissions. Plaintiff and
5 Pennsylvania Class Members did rely on Magellan Health’s misrepresentations and
6 omissions relating to its data privacy and security.

7 225. Plaintiff and Pennsylvania Class Members acted reasonably in relying on
8 Magellan Health’s misrepresentations and omissions, the truth of which they could not
9 have discovered with reasonable diligence.

10 226. Had Magellan Health disclosed to Plaintiff and Pennsylvania Class
11 Members that its data security systems were not secure and, thus, were vulnerable to
12 attack, Plaintiff and Pennsylvania Class Members would not have given their data to
13 Magellan Health.

14 227. Magellan Health acted intentionally, knowingly, and maliciously in
15 violating the Pennsylvania UTPCPL, and recklessly disregarded consumers’ rights.

16 228. As a direct and proximate result of Magellan Health’s unfair methods of
17 competition and unfair or deceptive acts or practices, Plaintiff and Pennsylvania Class
18 Members have suffered and will continue to suffer damages, injury, ascertainable losses
19 of money or property, and monetary and non-monetary damages as described above.

20 229. Plaintiff and Pennsylvania Class Members seek relief under 73 Pa. Stat. §
21 201-9.2, including, but not limited to, actual damages, treble damages, statutory damages,
22 injunctive relief and/or attorney’s fees and costs.

23 230. Plaintiff and Pennsylvania Class Members are also entitled to injunctive
24 relief requiring Defendant to, *e.g.*, (a) strengthen its data security systems and monitoring
25 procedures; (b) submit to future annual audits of those systems and monitoring
26 procedures; and (c) continue to provide adequate credit monitoring to all Pennsylvania
27 Class Members.

28 //

TENTH CAUSE OF ACTION
VIOLATION OF VIRGINIA PERSONAL INFORMATION BREACH
NOTIFICATION ACT, VA. CODE. ANN. § 18.2-186.6, et seq.

(On Behalf of Plaintiff Flanders and the Virginia Subclass)

231. Plaintiff restates and realleges paragraphs 1 through 112 as if fully set forth herein.

232. Defendant is required to accurately notify Plaintiff Mitchell Flanders and all Virginia Class Members without unreasonable delay under Va. Code Ann. § 18.2-186.6(B) following discovery or notification of a breach of its data security systems if unencrypted or unredacted PII and PHI was or is reasonably believed to have been accessed and acquired by an unauthorized person and causes, or Defendant reasonably believes has caused or will cause, identify theft or another fraud to Plaintiff Mitchell Flanders and/or any member of the Virginia Subclass.

233. The Defendant and its subsidiaries are entities that own, license, or maintain computerized data that includes Personal Information as defined by Va. Code Ann. §§ 18.2-186.6(B), (D).

234. Plaintiff's and Virginia Class Members' PII and PHI includes Personal Information as covered under Va. Code Ann. § 18.2-186.6(A).

235. Because Defendant discovered a breach of its security systems in which unencrypted or unredacted PII and PHI was or is reasonably believed to have been accessed and acquired by an unauthorized person, who will, or who it is reasonably believed will, engage in identify theft or another fraud, Defendant had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Va. Code Ann. §§ 18.2-186.6(B), (D).

236. By failing to disclose the Data Breach in a timely and accurate manner, Defendant violated Va. Code Ann. §§ 18.2-186.6(B), (D).

237. As a direct and proximate result of Defendant's violations of Va. Code Ann. §§ 18.2-186.6(B), (D), Plaintiff Mitchell Flanders and Virginia Class Members suffered damages, as described above.

1 246. Magellan Health’s unfair or deceptive acts or practices were likely to and
2 did in fact deceive reasonable consumers, including Plaintiff and Wisconsin
3 Class Members, about the true nature of its computer and data security and the quality of
4 the Magellan Health brand.

5 247. Magellan Health intentionally and knowingly misrepresented material facts
6 regarding the security and integrity of its data systems cyber-security protocols with an
7 intent to mislead Plaintiff and Wisconsin Class Members.

8 248. Magellan Health knew or should have known that its conduct violated Wis.
9 Stat. § 100.18.

10 249. As alleged above, Magellan Health made material statements about its
11 cyber-security protocols, the integrity of its data systems, and the maintenance of PII that
12 were either false or misleading.

13 250. Magellan Health owed Plaintiff and Wisconsin Class Members a duty to
14 disclose the true nature of the security of its computer and data systems and robustness
15 of its cyber-security protocols and practices because Magellan Health:

- 16 a. Possessed exclusive knowledge regarding the lack of security of its
17 employees’ PII;
- 18 b. Intentionally concealed the foregoing from Plaintiff and Wisconsin
19 Class Members; and/or
- 20 c. Made incomplete representations about the security and integrity of
21 its computer and data systems and cyber-security practices.

22 251. Magellan Health’s fraudulent claims of computer and data security and the
23 true nature of the security of such systems were material to Plaintiff and Wisconsin
24 Class Members.

25 252. Plaintiff and Wisconsin Class Members suffered ascertainable loss caused
26 by Magellan Health’s misrepresentations and its concealment of and failure to disclose
27 material information. Wisconsin Class Members would not have had their PII
28

1 compromised and would have taken steps to prevent identity theft and other harms, but
2 for Magellan Health’s violations described herein.

3 253. Magellan Health had an ongoing duty to all Magellan Health’s employees
4 – past and present – as well as members who received benefits from any one of the health
5 plans that is administered, to refrain from unfair and deceptive practices under Wis. Stat.
6 § 100.18.

7 254. All Wisconsin Class Members suffered ascertainable loss, including in the
8 form of out of pocket expenses and lost time to implement and maintain credit freezes
9 and identity theft prevention as a result of Magellan Health’s deceptive and unfair acts
10 and practices made in the course of its business.

11 255. Magellan Health’s violations present a continuing risk to Plaintiff
12 and Wisconsin Class Members as well as to the general public.

13 256. As a direct and proximate result of Magellan Health’s violations of Wis.
14 Stat. § 100.18, Plaintiff and Wisconsin Class Members have suffered injury-in fact and/or
15 actual damage.

16 257. Plaintiff and Wisconsin Class Members are entitled to damages and other
17 relief provided for under Wis. Stat. § 100.18(11)(b)(2).

18 258. Because Magellan Health’s conduct was committed knowingly and/or
19 intentionally, Plaintiff and Wisconsin Class Members are entitled to treble damages.

20 259. Plaintiff and Wisconsin Class Members also seek court costs and
21 attorneys’ fees under Wis. Stat. § 100.18(11)(b)(2).

22 260. Plaintiff and Wisconsin Class Members are also entitled to injunctive relief
23 requiring Defendant to, *e.g.*, (a) strengthen its data security systems and monitoring
24 procedures; (b) submit to future annual audits of those systems and monitoring
25 procedures; and (c) continue to provide adequate credit monitoring to all Wisconsin Class
26 Members.

27 ///

28 //

1 WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly
2 situated, respectfully request the following relief:

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

24
25 **DEMAND FOR JURY TRIAL**

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

1 Dated: October 29, 2020

Respectfully submitted,

2 **ZIMMERMAN REED LLP**

3 By: s/ Hart L. Robinovitch
4 Hart L. Robinovitch (AZ SBN 020910)
5 14646 North Kierland Blvd., Suite 145
6 Scottsdale, AZ 85254
7 Telephone: (480) 348-6400
8 Facsimile: (480) 348-6415
9 Email: hart.robinovitch@zimmreed.com

8 **BONNETT, FAIRBOURN,
9 FRIEDMAN & BALINT, P.C.**

10 Elaine A. Ryan (AZ Bar #012870)
11 Carrie A. Laliberte (AZ Bar #032556)
12 2325 E. Camelback Rd., Suite 300
13 Phoenix AZ 85016
14 Telephone: (602) 274-1100
15 Email: eryl@bffb.com
16 claliberte@bffb.com

15 **BONNETT, FAIRBOURN,
16 FRIEDMAN & BALINT, P.C.**

17 Patricia N. Syverson (AZ Bar #020191)
18 600 W. Broadway, Suite 900
19 San Diego, California 92101
20 Telephone: (619) 798-4593
21 Email: psyverson@bffb.com

21 *Additional counsel:*

22 **MASON LIETZ & KLINGER LLP**

23 Gary E. Mason*
24 David K. Lietz*
25 5301 Wisconsin Ave, NW
26 Suite 305
27 Washington, DC 20016
28 Telephone: (202) 429-2290
Email: gmason@masonllp.com
Email: dlietz@masonllp.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

**MORGAN & MORGAN
COMPLEX LITIGATION GROUP**

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

MASON LIETZ & KLINGER LLP

Gary M. Klinger*
227 W. Monroe Street, Suite 2100
Chicago, IL 60630
Telephone: (312) 283-3814
Email: gklinger@masonllp.com

RHINE LAW FIRM, P.C.

Joel R. Rhine**
Martin A. Ramey**
Janet R. Coleman**
1612 Military Cutoff Rd., Suite 300
Wilmington, NC 28403
Telephone: (910) 772-9960
Email: jrr@rhinelawfirm.com
mjr@rhinelawfirm.com

BERGER MONTAGUE PC

Michael Dell'Angelo**
1818 Market Street, Suite 3600
Philadelphia, PA 19103
Telephone: (215) 875-3000
Email: mdellangelo@bm.net

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

KEHOE LAW FIRM, P.C.

Michael K. Yarnoff**
Two Penn Center Plaza
1500 JFK Boulevard, Suite 1020
Philadelphia, PA 19102
Telephone: (215) 792-6676
Email: myarnoff@kehoelawfirm.com

DEYOUNG & ASSOCIATES

Neal A. DeYoung*
One Reservoir Office Park
Southbury, Ct. 06488
Telephone: (203) 731-7558
Email: neal@deyounglegal.com

Counsel for Plaintiff and the Putative Class

* *Previously admitted pro hac vice*
** *Pro hac vice to be filed*

EXHIBIT A



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

May 15, 2020



F5300-L01-0030277 P003 T00074 *****ALL FOR AADC 630

CHRIS A GRIFFEY

WILDWOOD, MO



Dear Chris A Griffey:

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

What Happened

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

What Information Was Involved

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

What We Are Doing

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

8621 Robert Fulton Drive, Columbia, MD 21046
www.magellanhealth.com

0030277



F5300-L01

What You Can Do

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

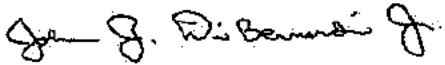
- Ensure that you enroll by: August 31, 2020 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your activation code: [REDACTED]

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

For More Information

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

Sincerely,



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

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

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

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

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

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

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

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

Reporting of identity theft and obtaining a police report.

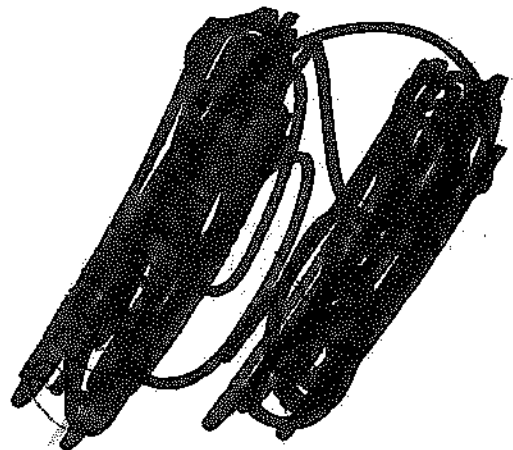
You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

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

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

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

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



Information About Identity Theft Protection Guide

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

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

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

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

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

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

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

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

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

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



EXHIBIT B



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

May 12, 2020



F5229-L01-0014194 P003 T00043 ALL FOR AADC 370

BHARATH MADURANTHAGAM RAYAM

NASHVILLE TN



Dear Bharath Rayam:

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

What Happened

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

What Information Was Involved

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

What We Are Doing

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

8621 Robert Fulton Drive, Columbia, MD 21046
www.magellanhealth.com



F5229-L01

Information About Identity Theft Protection Guide

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

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

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

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

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

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

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

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

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

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



EXHIBIT C

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

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

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

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

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

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



Dear Former Magellan Health Employee:

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

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

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

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

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

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

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

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

John DiBernardi
Chief Compliance Officer

Former Employee Q&A

Exactly what was stolen and how did it happen?

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

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

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

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

How many Magellan employees were impacted?

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

How was my information (SSN) stolen?

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

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

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

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

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

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

What are you doing to protect my financial data?

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

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

What should I do to protect my financial data?

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

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

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

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

Is my financial information being sold?

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

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

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

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

Should I contact the IRS?

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

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

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

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

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

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

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

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

Where can I learn more information?

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

© 2020 Magellan Health, Inc.

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



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



EXHIBIT D



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

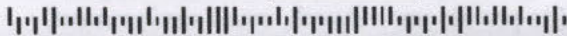
June 26, 2020



F6174-L02-0182425 P010 T00468 *****ALL FOR AADC 125

LAURA A LEATHER

DOVER PLAINS, NY



Dear Laura A Leather:

Magellan Health Inc.¹ (“Magellan”) was recently the victim of a criminal ransomware attack. We are writing to let you know how this incident may have affected your personal information and, as a precaution, to provide steps you can take to help protect your information. We take the privacy and security of your personal information very seriously and we sincerely regret any concern this incident may cause you.

Why Does Magellan Have My Personal Information

Magellan provides services for managing healthcare delivery, employee assistance program services, and pharmacy management services. Magellan's customers include health plans and other managed care organizations, employers, labor unions, various military and governmental agencies and third-party administrators. We also manage health services to individuals enrolled in our Medicaid and Medicare programs. We may have your information because of the services we provide to your employer or health plan, or to you directly.

What Happened

On April 11, 2020, Magellan discovered it was targeted by a ransomware attack. The unauthorized actor gained access to Magellan's systems after sending a phishing email on April 6 that impersonated a Magellan client. Once the incident was discovered, Magellan immediately retained a leading cybersecurity forensics firm, Mandiant, to help conduct a thorough investigation of the incident. The investigation revealed that this incident may have affected your personal information. At this point, we are not aware of any fraud or misuse of any of your personal information as a result of this incident, but we are notifying you out of an abundance of caution.

¹ Magellan Health, Inc. subsidiaries include but are not limited to: Magellan Healthcare, Inc., National Imaging Associates, Inc., Magellan Rx Management, LLC, Magellan Rx Pharmacy, LLC, Magellan Complete Care of Virginia, LLC, Florida MHS, Inc. d/b/a Magellan Complete Care of Florida, Magellan Complete Care of Arizona, Inc., Magellan Complete Care of Louisiana, Inc., Armed Forces Services Corporation, The Management Group, LLC, Senior Whole Health, LLC, Senior Whole Health of New York, Inc., 4-D Pharmacy Management Systems, LLC, Magellan Medicaid Administration, Inc., Magellan Pharmacy Solutions, Inc., Merit Health Insurance Company, VRx, LLC, and VRx Pharmacy, LLC
8621 Robert Fulton Drive. Columbia, MD 21046

0182425



F6174-L02

What Information Was Involved

The personal information accessed by the unauthorized actor included your Social Security number and/or other financial information and possibly included names and one or more of the following: date of birth, treatment information, health insurance account information, member ID, other health-related information, email addresses, phone numbers, and physical addresses. Again, we do not believe that any information has been used inappropriately.

What We Are Doing

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

What You Can Do

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

- Ensure that you enroll by: September 30, 2020 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your activation code: [REDACTED]

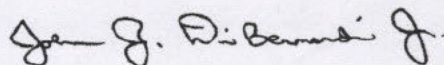
If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 888-451-6558 by September 30, 2020. Be prepared to provide engagement number DB20851 as proof of eligibility for the identity restoration services by Experian.

Keep a copy of this letter for your records in case of any potential future problems with your health plan benefit or other records. Review any statements you receive pertaining to your health plan benefits regularly and carefully; if you see indications of any treatment or services that you believe you did not seek or receive, call the number on your member ID card.

For More Information

The security of your personal information is important to us and we sincerely regret that this incident occurred. For more information, or if you have any questions or need additional information, please contact 888-451-6558.

Sincerely,



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

What Information Was Involved

The personal information accessed by the unauthorized actor included your Social Security number and/or other financial information and possibly included names and one or more of the following: date of birth, treatment information, health insurance account information, member ID, other health-related information, email addresses, phone numbers, and physical addresses. Again, we do not believe that any information has been used inappropriately.

What We Are Doing

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

What You Can Do

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

- Ensure that you enroll by: September 30, 2020 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your activation code: XPQF5CBF7

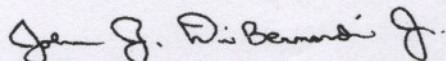
If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 888-451-6558 by September 30, 2020. Be prepared to provide engagement number DB20851 as proof of eligibility for the identity restoration services by Experian.

Keep a copy of this letter for your records in case of any potential future problems with your health plan benefit or other records. Review any statements you receive pertaining to your health plan benefits regularly and carefully; if you see indications of any treatment or services that you believe you did not seek or receive, call the number on your member ID card.

For More Information

The security of your personal information is important to us and we sincerely regret that this incident occurred. For more information, or if you have any questions or need additional information, please contact 888-451-6558.

Sincerely,



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

EXHIBIT E



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

July 21, 2020

F6559-L69-0032514 P003 T00079 *****ALL FOR AADC 852
CLARA WILLIAMS



APACHE JUNCTION, AZ



Dear Clara Williams:

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

What Happened

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

What Information Was Involved

The exfiltrated records include personal information such as your name and one or more of the following: date of birth, email address, physical address, W-2 or 1099 details such as your Social Security number or Taxpayer ID number, or health-related information including treatment information, health insurance account information, and member ID.

What We Are Doing

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



2

What You Can Do

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

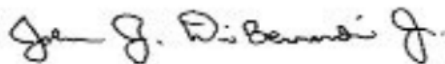
- Ensure that you enroll by: October 31, 2020 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your activation code: [REDACTED]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 888-451-6558 by October 31, 2020. Be prepared to provide engagement number DB21371 as proof of eligibility for the identity restoration services by Experian.

For More Information

The security of your personal information is important to us and we sincerely regret that this incident occurred. For more information, or if you have any questions or need additional information, please contact me at compliance@magellanhealth.com or Experian's call center at 888-451-6558.

Sincerely,



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

3

Information About Identity Theft Protection Guide

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

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

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

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

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

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

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

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

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

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



4

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

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

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

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

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

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

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

Reporting of identity theft and obtaining a police report.

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

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

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

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

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

EXHIBIT F



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

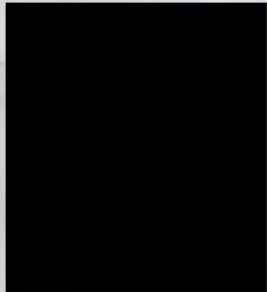
May 15, 2020



F5300-L01-0071139 P005 T00180 *****ALL FOR AADC 932

DANIEL A RANSON

MAMMOTH LAKES, CA [REDACTED]



Dear Daniel A Ranson:

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

What Happened

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

What Information Was Involved

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

What We Are Doing

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



additional steps you may take to help protect yourself, including recommendations from the Federal Trade Commission regarding identity theft protection and details regarding placing a fraud alert or a security freeze on your credit file. As an added precaution, to help protect your identity, we are offering a complimentary three-year membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

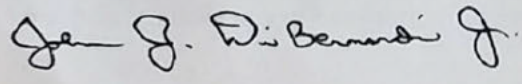
- Ensure that you enroll by: August 31, 2020 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your activation code: [REDACTED]

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

For More Information

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

Sincerely,



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Reporting of identity theft and obtaining a police report.

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

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

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

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

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

EXHIBIT G

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

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



John DiBernardi
SVP, Chief Compliance Officer

Dear Former Magellan Health Employee:

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

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

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

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

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

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

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

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

John DiBernardi
Chief Compliance Officer

Former Employee Q&A

Exactly what was stolen and how did it happen?

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

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

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

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

How many Magellan employees were impacted?

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

How was my information (SSN) stolen?

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

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

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

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

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

- Equifax: [Equifax.com](https://www.equifax.com) or 1-800-685-1111

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

What are you doing to protect my financial data?

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

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

What should I do to protect my financial data?

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

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

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

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

Is my financial information being sold?

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

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

We have no reason to believe your information has been used inappropriately. If you believe your personal information has been misused, visit the FTC's site at [IdentityTheft.gov](https://www.ftc.gov/identity-theft) to get recovery steps and to file an identity theft complaint. Your complaint will be added to the FTC's Consumer Sentinel Network, where it will be accessible to law enforcers for their investigations.

Should I contact the IRS?

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

- If you received an [IRS 5071C](https://www.irs.gov/irs5071c) or an [IRS 5747C](https://www.irs.gov/irs5747c) letter; call the number provided in the notice or, if instructed, visit the IRS's Identity Verification Service at https://go.magellanhealth.com/e/703943/ud-scams-identity-verification/hbglz/100020631?h=TR0-EvEqU_MWiVQyZm2IU4eDcS3LNgc-4cKFByz35DM.

- Complete IRS Form 14039, Identity Theft Affidavit, if your e-filed return is rejected because of a duplicate filing under your SSN or you are otherwise instructed to do so.

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

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

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

- If instructed, visit the IRS's Identity Verification Service at https://go.magellanhealth.com/e/703943/ud-scams-identity-verification/hbglz/100020631?h=TR0-EvEqU_MWiVQyZm2IU4eDcS3LNgc-4cKFByz35DM.
- Complete IRS Form 14039, Identity Theft Affidavit, if your e-filed return is rejected because of a duplicate filing under your SSN or you are otherwise instructed to do so.

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

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

Where can I learn more information?

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

© 2020 Magellan Health, Inc.

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



<https://go.magellanhealth.com/unsubscribe/u/703943/0a2050114586c65f40dc4da7db1e0a5d4b7ef8d50df0023662c7fba0b139015/100020631>

EXHIBIT H

What You Can Do

Please review the "Information About Identity Theft Protection" reference guide, enclosed here, which describes additional steps you may take to help protect yourself, including recommendations from the Federal Trade Commission regarding identity theft protection and details regarding placing a fraud alert or a security freeze on your credit file.

As an added precaution, to help protect your identity, we are offering a complimentary two-year membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you enroll by: September 30, 2020 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3heredit>
- Provide your activation code: [REDACTED]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 888-451-6558 by September 30, 2020. Be prepared to provide engagement number DB20695 as proof of eligibility for the identity restoration services by Experian.

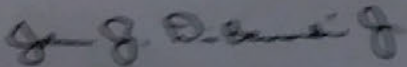
In addition, please be on the lookout for any scams that attempt to lure you into providing personal information in connection with this incident. Magellan will NOT call you or send you any email messages asking for your personal information or credit card information, or send you any email messages asking you to "click" on any links to activate identity theft protection services. You should not provide information in response to any such calls or email messages, and you should not click on any links within any such email messages. The ONLY ways to set up the credit monitoring we have obtained for you or to contact Experian are set forth in this letter.

Keep a copy of this letter for your records in case of any potential future problems with your health plan benefit or other records. Review any statements you receive pertaining to your health plan benefits regularly and carefully; if you see indications of any treatment or services that you believe you did not seek or receive, call the number on your member ID card.

For More Information

The security of your personal information is important to us and we sincerely regret that this incident occurred. For more information, or if you have any questions or need additional information, please contact 888-451-6558.

Sincerely,



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

* Online members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an American company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

EXHIBIT I

Magellan
HEALTH.

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

First Letter

F6003-L05-0011867 P003 T00031 *****ALL FOR AADC 370

TERESA CULBERSON

COLUMBIA, TN



Dear Teresa Culberson:

We take privacy and security very seriously, so we are contacting you about a data breach that has happened. The data breach may have included some of your information with Magellan Health Inc.¹ ("Magellan"). This letter tells you how some information about you may have been put at risk.

What Happened

On [REDACTED], we learned that we had a data breach. This happened when an unknown person may have gotten into some email accounts and a computer system that stores files. The email accounts and computer system may have your information in them. We do not think the person had a plan to do anything with your information.

What Information Was Involved

The emails and server had information such as:

- Name
- Birthday
- Address
- Email
- Medical information

What We Are Doing

When we found out about this we:

- Started an investigation
- Told the FBI
- Created new ways to make our security better

¹ Magellan Health, Inc. subsidiaries include but are not limited to: Magellan Healthcare, Inc., National Imaging Associates, Inc., Magellan Rx Management, LLC, Magellan Rx Pharmacy, LLC, Magellan Complete Care of Virginia, LLC, Florida MHS, Inc. d/b/a Magellan Complete Care of Florida, Magellan Complete Care of Arizona, Inc., Magellan Complete Care of Louisiana, Inc., Armed Forces Services Corporation, The Management Group, LLC, Senior Whole Health, LLC, Senior Whole Health of New York, Inc., 4-D Pharmacy Management Systems, LLC, Magellan Medical Administration, Inc., Magellan Pharmacy Solutions, Inc., Merit Health Insurance Company, VRx, LLC, and VRx Pharmacy, LLC.

Si requiere asistencia en español, por favor llame al 888-451-6558.



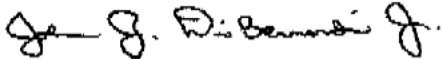
What You Can Do

- Review the attached guide to learn how to protect yourself
- Keep this letter in a safe place in case you need it later
- Check your mail for things that don't look right
- If you see something wrong in anything we send you, report it to us right away

For More Information

You can call us with any questions at ~~800-451-6558~~. Be prepared to provide engagement number [REDACTED] as proof of eligibility for the identity restoration services by Experian.

Sincerely,



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

Information About Identity Theft Protection Guide

Fraud Alert

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

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

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

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

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

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

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

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

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



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

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

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

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

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

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

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

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

Reporting of identity theft and obtaining a police report.

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

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

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

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

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

Magellan Rx Medicare

Prescription ID Card

RxBIN: [REDACTED]
RxPCN: [REDACTED]
RxGrp: [REDACTED]
Issuer: [REDACTED]

ID No. [REDACTED]
Name **Teresa Culberson**

<http://medicare.magellanrx.com>

MedicareRx
Prescription Drug Coverage

S4607/012

Patient Customer Service: 800-424-5870
TTY: 711

Pharmacist Use Only: 800-424-5870

Submit Medicare Part D Claims to:
Magellan Rx Medicare
PO Box 1433
Maryland Heights, MO 63043