

Exhibit A4

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

6 Hart L. Robinovitch (AZ SBN 020910)
7 **ZIMMERMAN REED LLP**
8 14646 North Kierland Blvd., Suite 145
9 Scottsdale, AZ 85254
10 Telephone: (480) 348-6400
11 Facsimile: (480) 348-6415
12 Email: hart.robinovitch@zimmreed.com

10 *Attorneys for Plaintiffs and the Class*
11 *(Additional Counsel listed below)*

13 **UNITED STATES DISTRICT COURT**
14 **DISTRICT OF ARIZONA**

15 Chris Griffey, et al.,
16 Plaintiffs,
17 v.
18 Magellan Health, Incorporated,
19 Defendant.

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

**SECOND AMENDED
CONSOLIDATED CLASS ACTION
COMPLAINT**

DEMAND FOR JURY TRIAL

(Assigned to the Honorable Michael T. Liburdi)

22 Daniel Ranson, et al.,
23 Plaintiffs,
24 v.
25 Magellan Health, Incorporated,
26 Defendant.
27

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

10 **PARTIES**

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

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

22 3. As a result of the Data Breach, Plaintiff Rayam learned that an unauthorized
23 and fraudulent charge in the amount of \$3.79 was made to his credit card. While not a
24 significant sum, Plaintiff Rayam is informed and believes that the charge was an attempt
25 to test whether his account remained open for possibly a larger withdrawal later. As a
26 result of that charge, Plaintiff Rayam was required to report the issue to the bank that
27 issued the card and to request a new card. Around the same time, Plaintiff Rayam began
28 receiving spam telephone calls and spam text messages daily, which even interrupt him

1 while he is at work. As a result of those calls, and Plaintiff Rayam's efforts to block
2 them, he has blocked nearly 500 numbers from calling his phone.

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

8 5. Plaintiff Laura Leather is, and at all times mentioned herein was, a citizen
9 of the state of New York residing in the city of Dover Plains. Upon information and
10 belief, Magellan Health provided services to Plaintiff Leather's employer and/or to her
11 health plan. Plaintiff Leather received notice of the Data Breach, and a copy of the notice
12 is attached hereto as Exhibit D. As a result of the Data Breach, Plaintiff Leather has taken
13 responsive measures such as individually paying for Lifelock Standard credit monitoring
14 and protection service, something that she otherwise would not have incurred to ensure
15 that her identity is not stolen and that her personal affairs are not further compromised.
16 The Lifelock Standard credit monitoring service has a monthly cost of \$9.99, and is
17 superior to the Experian IdentityWorks 3b product offered by Defendant, in that the
18 Lifelock service provides monitoring and alerts if it detects Plaintiff Leather's: A)
19 Personal Info on Service and Credit Applications; B) Personal Information on the Dark
20 Web; C) USPS Address Change Verification, and D) Fake Personal Information
21 Connected to her identity.¹ By contrast, the Experian IdentityWorks product offered by
22 Defendant provides none of these services.² In addition, since the breach, she has learned
23 that her e-mail and phone number were made available on the "Dark Web" and she has
24 been receiving deeply disturbing pornographic texts. These events did not occur prior to
25 the Data Breach. She also has noticed a marked increase in spam calls to her cell phone,
26 As a result, she has spent many hours trying to block calls and attempts to text her, as

27
28 ¹ <https://www.lifelock.com/products/> (last visited October 11, 2021)

² <https://www.experianidworks.com/3bcredit> (last visited October 11, 2021).

1 well as remains worried and stressed that a hacker will use her information to inflict
2 further damage to her credit and to her pocketbook.

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

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

19 8. Plaintiff Daniel Ranson is, and at all times mentioned herein was, a citizen
20 and resident of California. Plaintiff Ranson is a licensed clinical social worker in
21 California and currently practices as a psychotherapist in Mammoth Lakes, California.
22 At the time of the Data Breach, Plaintiff had contracted with Magellan to treat behavioral
23 health patients with Human Affairs International of California ("HAIC"), a wholly owned
24 subsidiary of Magellan Healthcare, Inc., which serves as a mental health service
25 administrator ("MHSA") for Blue Shield of California, Blue Shield Life & Health
26 Insurance Company, and other health plans.³ Plaintiff Ranson received written notice of

27 _____
28 ³ As an MHSA, Magellan manages healthcare services for approximately 40 million
members nationwide, which includes the offering of provider networks.

1 the Data Breach, and a true and correct copy of that Notice is attached hereto as Exhibit
2 F.

3 9. As a result of the Data Breach, Plaintiff Ranson enrolled in a credit
4 monitoring service to protect himself against the unauthorized use of his data, and he
5 changed passwords associated with his online accounts. The monitoring service Plaintiff
6 Ranson enrolled in was necessary given the sensitive nature of the information
7 compromised by the Breach and the fact that the product offered by Defendant did not
8 offer identity theft monitoring and protection. As a health care provider with a busy
9 practice, Plaintiff Ranson had to take time away from his practice to review his credit
10 reports and accounts. He still scrutinizes all his accounts on a level much greater than
11 before the Data Breach. Following the filing of his complaint in his related case, *Ranson*
12 *v. Magellan Health*, No. CV-20-01350-PHX-MTL (D. Ariz.), a thief who had obtained
13 his private information as a result of the Data Breach was able to successfully open an
14 account with AT&T under Ranson's name. As a direct and proximate result of that
15 fraudulent account opening, Plaintiff Ranson was required to spend considerable time
16 trying to resolve the problem – time that he could have spent on other aspects of his
17 professional and personal life. He likewise suffered the erroneous reporting of that
18 account to his credit report.

19 10. Shortly after the filing of his complaint, the Defendant notified Plaintiff
20 Ranson that it was going to perform an audit of his billing and treatment, only to rescind
21 that notification audit later that same day. Plaintiff Ranson is informed and believes that
22 the audit was prompted by his participation in this lawsuit.

23 11. Plaintiff Mitchell Flanders is, and at all times mentioned herein was, a
24 citizen and resident of Virginia. In 2018, Plaintiff Flanders worked as an intern for
25 Magellan Federal (formerly the Armed Forces Services Corporation), another Magellan
26 subsidiary, prior to being promoted to a full-time position, where he worked until his
27 resignation from the company in 2019. He is currently unaffiliated with Magellan.
28 Plaintiff Flanders received written notice of the Data Breach, and a true and correct copy

1 of that notice is attached hereto as Exhibit G. As a result of the Data Breach, Plaintiff
2 Flanders has increased the time spent monitoring his accounts, and recently paid a
3 cybersecurity consultant to search the “Dark Web” for his information following the
4 breach, and the consultant discovered that his Social Security Number had indeed been
5 exposed and was available for purchase on the black market. This expense was necessary
6 given the sensitive nature of the information compromised by the Breach and the fact that
7 the monitoring services offered by Defendant do not include identity theft monitoring
8 and protection.

9 12. Plaintiff Joseph Rivera is, and at all times mentioned herein was, a citizen
10 and resident of Wisconsin. Plaintiff Rivera was employed by Abbott Laboratories from
11 May 2001 through May 2012. In 2012, Abbott Laboratories split into two divisions, and
12 Plaintiff Rivera became an employee of Abvie and continues to be employed with Abvie.
13 During the time that Plaintiff Rivera was employed by Abbot Laboratories (May 2001-
14 May 2012), Magellan Health administered Abbott Laboratories’ health care plan in which
15 Plaintiff Rivera was a participant. Plaintiff Rivera received written notice of the Data
16 Breach by letter dated June 18, 2020, and a true and correct copy of that notice letter is
17 attached hereto as Exhibit H.

18 13. Plaintiff Teresa Culberson is, and at all times mentioned herein was, a
19 citizen and resident of Tennessee. Plaintiff Culberson was an insured under Magellan’s
20 Rx Medicare program. On or about June 15, 2020, Plaintiff Culberson received a letter
21 from Magellan notifying her that her information was compromised as the result of an
22 April 11, 2020 Data Breach at Magellan, and a true and correct copy of that notice letter
23 is attached hereto as Exhibit I. Since the Data Breach, Plaintiff Culberson has had to
24 replace her ATM card three times and has had to stop auto billing from her cellphone and
25 insurance companies.

26 14. Plaintiff Keith Lewis is a citizen and resident to Florida. On or about July
27 24, 2020, Plaintiff Lewis received a notice from Magellan, like those received by the
28

1 other plaintiffs, that his information had been compromised during the Data Breach. A
2 true and correct copy of the notice sent to Plaintiff Lewis is attached hereto as Exhibit J.

3 15. At the time of the breach, Plaintiff Lewis had a free account with Experian
4 that provided a very basic level of monitoring his credit report. Upon receiving the notice,
5 and because he was concerned that his data had been stolen, he upgraded from the free
6 service to a more robust plan, which costs \$24.99 monthly and is superior to the product
7 offered by Defendant, which does not offer identity theft monitoring and protection.
8 Recently, he has received several e-mails from the service about various “hits” to his
9 credit. For example, he had 13 unfamiliar accounts go to collections. As a result, he has
10 spent and continues to spend significant time disputing and attempting to resolve the
11 fraudulent accounts. In addition, he had both his Chase and Bank of American checking
12 accounts involuntarily closed due to repeated suspicious activity within the last two
13 months and, consequently, he had to open new accounts. He received two debit cards in
14 the mail from GreenDot even though he did not apply for them. And, his mother, whose
15 number was associated with his protected health information, has also received
16 suspicious phone calls referencing her son, where the caller repeatedly attempts to send
17 the mother a delivery on behalf of Plaintiff Lewis and asks his mother to confirm her
18 son’s address and date of birth. Plaintiff attributes all this activity to the Data Breach.

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

23 **JURISDICTION AND VENUE**

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

1 18. This Court has jurisdiction over Defendant, which operates and is
2 headquartered in this District. The computer systems implicated in this Data Breach are
3 also likely based in this District. Through its business operations in this District, Magellan
4 and its related subsidiaries intentionally avail themselves of the markets within this
5 District to render the exercise of jurisdiction by this Court just and proper.

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

13 **NATURE OF THE ACTION**

14 20. This class action arises out of the most recent Data Breach involving
15 Defendant and its subsidiaries and affiliates.⁴ As a result of the Data Breach, the PII and
16 PHI of Plaintiffs and at least 365,000 Class Members is in the hands of cyberthieves.
17 Plaintiffs and Class Members suffered ascertainable losses in the form of out-of-pocket
18 expenses and the value of their time reasonably incurred to remedy or mitigate the effects
19 of the attack. In addition, Plaintiffs’ and Class Members’ sensitive personal
20 information—which was entrusted to Magellan Health, its officials and agents—was
21 compromised and unlawfully accessed due to the Data Breach. Information
22 compromised in the Data Breach included names, contact information, employee ID
23 numbers, and W-2 or 1099 information, including Social Security Numbers or taxpayer

24 ⁴ 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), Magellan Healthcare of
28 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 identification numbers, treatment information, health insurance account information,
2 member IDs, other health-related information, email addresses, phone numbers, physical
3 addresses, and additional PII.

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

10 22. Defendant maintained the PII and PHI of its employees and health plan
11 participants in a reckless and negligent manner. In particular, the PII and PHI was
12 maintained on Defendant's computer network in a condition vulnerable to cyberattacks.
13 For example, Defendant failed to monitor ingress and egress network traffic; failed to
14 maintain an inventory of public facing IPs; failed to monitor elevated privileges; failed
15 to equip its server with anti-virus or anti-malware; and failed to employ basic file integrity
16 monitoring. The mechanism of the cyberattack and potential for improper disclosure of
17 Plaintiffs' and Class Members' PII and PHI was a known risk to Defendant, as it was
18 subject to another Data Breach a mere 11 months prior that involved a similar phishing
19 attack. Thus, Defendant was on notice that failing to take steps necessary to secure the
20 PII and PHI from those risks left that property in a dangerous condition.

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

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

28

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

9 26. As a direct and proximate result of the Data Breach, Plaintiffs and Class
10 Members have suffered and will continue to suffer damages and economic losses in the
11 form of: 1.) having fraudulent charges and debits applied to their personal accounts; 2.)
12 losses incurred as a result of paying for credit monitoring and fraud alert services; and 3.)
13 the loss of time needed to: take appropriate measures to avoid unauthorized and
14 fraudulent charges; change their usernames and passwords on their accounts; investigate,
15 correct and resolve unauthorized debits, charges, and fees charged against their accounts;
16 deal with spam messages and e-mails received as a result of the Data Breach; respond to
17 false unemployment claims; and file reports with both regulatory authorities and law
18 enforcement. Additionally, because Plaintiffs and Class Members have and will continue
19 to have erroneous information regarding fraudulent accounts and changes to their credit
20 reports, Plaintiffs and Class Members will have to not only spend time trying to resolve
21 those matters, but will suffer from lower credit scores and pay higher interest rates for
22 credit, ultimately paying more money than they would have prior to the Data Breach.
23 Plaintiffs and Class Members have likewise suffered and will continue to suffer an
24 invasion of their property interest in their own PII and PHI such that they are entitled to
25 damages for unauthorized access to and misuse of their PII and PHI from Defendant.
26 And, Plaintiffs and Class Members will suffer from future damages associated with the
27 unauthorized use and misuse of their PII and PHI as thieves will continue to use the
28 information to obtain money and credit in their name for several years. By their

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

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

7 28. Accordingly, Plaintiffs bring this action against Defendant seeking redress
8 for its unlawful conduct, and asserting claims for: (i) negligence; (ii) unjust enrichment;
9 (iii) violation of California's Unfair Competition Law; (iv) violation of California's
10 Consumer Privacy Act; (v) violation of New York's General Business Law § 349; (vi)
11 violation of Pennsylvania's Unfair and Deceptive Trade Practices and Consumer
12 Protection Law; (vii) violation of Wisconsin's Deceptive Trade Practices Act; and (viii)
13 violation of Florida's Deceptive and Unfair Trade Practices Act.

14 **STATEMENT OF FACTS**

15 ***A. Defendant Magellan Health***

16 29. Incorporated in 1969 in Delaware, Defendant Magellan Health is a for-
17 profit managed health care company focused on special populations, complete pharmacy
18 benefits, and other specialty areas of healthcare.

19 30. Defendant directly manages health benefits for its members' patients,
20 including those of its affiliates/subsidiaries Magellan Healthcare, Inc. (55,637 patients);
21 Merit Health Insurance Company (102,748 patients), Florida MHS, Inc. d/b/a Magellan
22 Complete Care of Florida (76,236 patients), the University of Florida Health Jacksonville
23 (54,002 patients), Magellan Healthcare of Maryland, LLC (50,410 patients), VRx
24 Pharmacy (33,040 patients), National Imaging Associates, Inc. (22,560 patients), UF
25 Health Shands (13,146 patients), UF Health (9,182 patients), and Magellan Complete
26 Care of Virginia, LLC (3,568 patients).

27 31. As part of its contractual relationship with the aforementioned
28 affiliates/subsidiaries and several other providers, Magellan administers the health and

1 pharmaceutical benefits offered by those affiliates/subsidiaries. Magellan Health
2 received fees from those affiliates or the states in which they operate to administer those
3 benefits and to provide services related to those benefits to Class Members, which
4 included storing Class Members' personal data on its computers and computer systems.
5 The fees received by Defendant for these services are accrued and paid as a result of
6 Class Members' participation in and payment for these health and pharmaceutical plans.

7
8
9 **B. *The Data Breach***

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

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

17 34. This was the second such data breach to occur at Magellan within the last
18 year, with notices of the breaches only surfacing within the last six months.

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

24 36. However, despite discovering the breach during the summer, Magellan did
25 not notify individuals affected by the first breach until November of 2019. A related
26 class action concerning that breach has been filed in the Maricopa County Superior Court
27
28

1 of Arizona, Case No. CV2020-013648, after being previously filed in this District,
2 *Dearing v. Magellan Health, Inc., et al.*, 2:20-cv-0-0747-SPL (D. Ariz.).⁵

3 37. During the more recent Data Breach, Magellan's servers were hit by a
4 ransomware attack. A ransomware attack deploys a type of malicious software that
5 blocks access to a computer system or data, usually by encrypting it, until the victim pays
6 a fee to the attacker.⁶

7 38. Magellan detected the ransomware attack on April 11, 2020 when files
8 were encrypted on its systems. An investigation into the attack allegedly revealed the
9 attacker had gained access to its systems following a response to a spear phishing email
10 sent on April 6.

11 39. A Magellan Health employee had inappropriately responded to the email
12 phishing scheme while the company was still managing the effects of the first breach,
13 allowing unauthorized actors to gain access to the employees' email accounts.

14 40. The Data Breach was a direct result of Defendant's failure to implement
15 adequate and reasonable cyber-security procedures and protocols necessary to protect PII
16 and PHI, including the PII of its employees (including Plaintiffs) and the PII and PHI of
17 participants in the health and pharmaceutical plans of the aforementioned
18 affiliates/subsidiaries. For example, Defendant failed to monitor ingress and ingress
19 network traffic; failed to maintain an inventory of public facing Ips; failed to monitor
20 elevated privileges; failed to equip its server with anti-virus or anti-malware; and failed
21 to employ basic file integrity monitoring.

22
23
24 _____
25 ⁵ The first Magellan case was dismissed as to the 44,000 TennCare beneficiaries for
26 failure to allege Article III standing. The case was refiled in state court under the more
27 liberal state law standing requirements. The facts and the alleged injuries of the first
28 Magellan (TennCare) complaint are distinct from those presented here.

⁶ *What Is Ransomware?* Proofpoint, <https://www.proofpoint.com/us/threat-reference/ransomware> (last visited October 28, 2020).

1 41. On or about May 12, 2020, more than a month after the attack, Magellan
2 Health notified affected persons and various governmental agencies of the Data Breach.
3 The Notice of Data Incident (“Notice”) stated, in relevant part:

4 **Notice of Data Incident**

5 *What Happened*

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

21 *What Information Was Involved*

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

26 *What We Are Doing*

27 Magellan immediately reported the incident to, and is working
28 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.⁷

⁷<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 became unavailable. An archived version of the

1 42. Upon information and belief, this notice was sent to 50,410 persons, and
2 was reported to the U.S. Department of Health and Human Services (“HHS”) on June
3 12, 2020.
4

5 43. On June 12, 2020, Defendant subsequently issued a second notice of Data
6 Breach to the plan participants of Complete Care of Florida and Magellan Rx Pharmacy
7 of Maryland and reported the Data Breach for Magellan Health to HHS. This notice was
8 sent to 76,236 plan participants of Complete Care of Florida, and 33,040 plan participants
9 of Magellan Rx Pharmacy of Maryland.
10

11 44. This second notice of Data Breach stated, in pertinent part:

12 *Notice of Security Incident*

13
14 Magellan Health, Inc. and its subsidiaries and affiliates
15 (“MAGELLAN”) recently discovered a ransomware attack.
16 We are providing notice of this incident, along with
background information of the incident and steps that those
affected can take.

17 *What Happened*

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

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

25
26 _____
27 above URL can be found on the Internet Archive, *available at*
28 [https://web.archive.org/web/20201005041745/https://oag.
ca.gov/system/files/MAGELLAN%20-%20Sample%20Individual%20Notice.pdf](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 Information Was Involved*

2 The personal information included names and one or more of
3 the following: treatment information, health insurance account
4 information, member ID, other health-related information,
5 email addresses, phone numbers, and physical addresses. In
6 certain instances, Social Security Numbers were also affected.

7 *What Are We Doing*

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

14 A copy of this second notice is posted on Defendant's website.⁸

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

20 46. On June 15, 2020, Defendant issued a notice identical in form to the June
21 12, 2020 notice to persons affected by this Data Breach who were plan participants of
22 Defendant's affiliate/subsidiary Magellan Complete Care of Virginia, LLC, and reported
23 the Data Breach for that affiliate to HHS on that same date.

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

26 48. The June 26, 2020 notice of Data Breach stated, in pertinent part:

27 Magellan Health, Inc. ("Magellan") was recently the victim of
28 a criminal ransomware attack. We are writing to let you know how
this incident may have affected your personal information and, as a

⁸ <https://www.magellanhealth.com/news/security-incident/> (last visited October 28, 2020).

1 precaution, to provide steps you can take to help protect your
2 information.

3 *What Happened*

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

14 *What Information Was Involved*

15 The personal information accessed by the unauthorized actor
16 included your Social Security number and/or other financial
17 information and possibly included names and one or more of the
18 following: treatment information, health insurance account
19 information, member ID, other health-related information, email
20 addresses, phone numbers, and physical addresses. In certain
21 instances, Social Security Numbers were also affected.

22 *What Are We Doing*

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

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

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

50. Due to its business and operations, Magellan is obligated by the Health
Insurance Portability and Accountability Act of 1996 ("HIPAA") to comply with a series

1 of administrative, physical security, and technical security requirements in order to
 2 protect sensitive patient information. Among other things, the law mandates Magellan
 3 develop, publish, and adhere to a privacy practice.

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

9 52. Defendant assures its patients, members, and other consumers that “[y]our
 10 personal privacy is important to us.”⁹ Magellan Health’s Privacy Policy further states:
 11 “Magellan uses physical, technical, and administrative safeguards to protect any
 12 personally identifiable data stored on its computers. Only authorized employees and third
 13 parties have access to the information you provide to Magellan for providing service to
 14 you.”¹⁰

15 53. Defendant further represents to its patients, members, and other consumers
 16 that:

17 Magellan has historically held the privacy of patient information as a key
 18 tenet of our operations and processes. Magellan has always implemented
 19 policies and procedures for confidentiality that met or exceeded existing state
 20 and federal regulations. Our many existing policies detailing compliance
 21 with HIPAA and all its implementing regulations (including the HITECH
 22 Act and the Omnibus Rule of 2013 as well) and other privacy-related
 23 requirements include:

- 24 • Authorization to Use and Disclose PHI (Protected Health Information)
- 25 • General Rules for Uses & Disclosures of PHI
- 26 • Uses & Disclosures of PHI for Treatment, Payment, & Health Care
 27 Operations

28 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).

¹⁰ *Id.*

- Oral & Written Transmission of PHI and Confidential Information
- Member Right to Request Privacy Protection of PHI
- Member Right to Request Access to PHI
- Member Right to Request Amendment of PHI
- Member Right to Request an Accounting of Disclosure of PHI
- Verification Policy
- Member Representation
- Notice of Privacy Practices
- Minimum Necessary Uses and Disclosures of PHI
- Uses & Disclosures of PHI Requiring No Permission From the Member
- Uses & Disclosures of PHI for Marketing, Fundraising, and Underwriting
- Uses & Disclosures for Specialized Government Functions
- Uses & Disclosures of PHI Requiring Prior Internal Approval
- Uses & Disclosures of PHI for Judicial & Administrative Proceedings
- Limited Data Set and De-Identification of PHI
- Unauthorized Uses & Disclosures of PHI¹¹

54. As such, Magellan recognizes its obligations under HIPAA to safeguard and protect patient PHI and PII. These obligations also extend to Magellan employees, as the company has an established Privacy Policy that details the types of PII and PHI Magellan collects from its employees, providers, and patients, among others.¹² Additionally, under various federal and state laws, regulations, industry practices and common law, Magellan is bound to safeguard and protect the personal data of its employees, providers, and patients to avoid unauthorized disclosure to third parties.

55. Also, all members of Magellan health plans are provided with their health plan's HIPAA Notice of Privacy Practices, which were disseminated to them in their home states, and that provides information and representations about how members' protected health information (PHI) is handled.

¹¹ <https://www.magellanhealth.com/about/compliance/hipaa/> (last visited October 11, 2021).

¹² <https://www.magellanhealth.com/privacy-policy/#:~:text=MAGELLAN%20uses%20physical%2C%20technical%2C%20and,for%20providing%20service%20to%20you> (last visited October 28, 2020).

1 56. For example, the Notice of Privacy Practices for Magellan Health Services
2 of California, Inc. – Employer Services “describes how your health information may be
3 used and disclosed.”¹³ It states that the “California companies affiliated with Magellan
4 Health Services listed above believe in protecting the privacy of your health
5 information,” and that “[w]e may use or disclose your Protected Health Information
6 (PHI) only for very specific reasons.” It further states that if Magellan needs to “use or
7 disclose information in a way that is not generally described in this notice, we will contact
8 you for your written permission before use or disclosure.” It represents that the “law
9 requires us to maintain the privacy of your PHI. The law also requires us to provide you
10 with this notice of our legal duties and privacy practices with respect to your PHI. We
11 are required to follow the terms of the privacy policy that is currently in effect.”

12 57. Upon information and belief, all of the Magellan health plans HIPAA
13 Notice of Privacy Practices contain the same or substantially similar representations and
14 promises to protect the privacy of patient/members’ PHI.

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

16 58. Data Breaches have become widespread and especially so in healthcare. In
17 2016, the number of U.S. Data Breaches surpassed 1,000, a record high representing a
18 40% increase in the number of Data Breaches from the previous year. In 2017, another
19 record high of 1,579 breaches were reported, representing a 44.7% increase over 2016.¹⁴
20 In 2018, there was an extreme jump of 126% in the number of consumer records exposed
21 from Data Breaches. In 2019, there was a 17% increase in the number of breaches (1,473)
22 over 2018, with 164,683,455 sensitive records exposed.¹⁵

23 ¹³ https://www.magellanassist.com/disclaimer/c_vista_capp.aspx (last visited October
24 11, 2021).

25 ¹⁴ Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review*,
<https://www.idtheftcenter.org/2017-data-breaches/> (last visited October 28, 2020).

26 ¹⁵ Identity Theft Resource Center *Identity Theft Resource Center’s Annual End-of-Year*
27 *Data Breach Report Reveals 17 Percent Increase in Breaches Over 2018*,
28 <https://www.idtheftcenter.org/identity-theft-resource-centers-annual-end-of-year-data->

1 59. Not surprisingly, companies in the business of storing and maintaining PII
2 and PHI, such as Magellan Health are among the most targeted—and therefore at risk—
3 for cyber-attacks.¹⁶

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

15 61. Phishing attacks are well understood by the cyberprotection community
16 and are generally preventable with the implementation of a variety of proactive measures
17
18
19

20
21

breach-report-reveals-17-percent-increase-in-breaches-over-2018/ (last visited October
22 28, 2020).

23 ¹⁶ Cyber Security Hub, *Top 8 Industries Reporting Data Breaches in The First Half Of*
24 *2019*, [https://www.cshub.com/attacks/articles/top-8-industries-reporting-data-breaches-](https://www.cshub.com/attacks/articles/top-8-industries-reporting-data-breaches-in-the-first-half-of-2019)
25 [in-the-first-half-of-2019](https://www.cshub.com/attacks/articles/top-8-industries-reporting-data-breaches-in-the-first-half-of-2019) (last visited October 28, 2020).

26 ¹⁷ *What is phishing? How this cyber attack works and how to prevent it*, CSO Online,
27 February 20, 2020, [https://www.csoonline.com/article/2117843/what-is-phishing-how-](https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html)
28 [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).

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

1 such as sandboxing inbound e-mail¹⁹, inspecting and analyzing web traffic, penetration
2 testing²⁰, and employee education, among others.

3 62. Among various data, healthcare related data is some of the most sensitive
4 and personally consequential when it is compromised. A report focusing on healthcare
5 breaches found that the “average total cost to resolve an identity theft-related
6 incident...came to about \$20,000,” and that the victims were often forced to pay out-of-
7 pocket costs for health care they did not receive in order to restore coverage.²¹ Almost
8 50% of the victims lost their health care coverage as a result of the incident, while nearly
9 one-third said their insurance premiums went up after the event. Forty percent of the
10 customers were never able to resolve their identity theft at all. Data breaches and identity
11 theft have a crippling effect on individuals and detrimentally impact the economy.²²

12 63. In recent years, the pace of breaches within healthcare organizations has
13 rapidly increased. According to a 2019 HIMSS Cybersecurity Survey, some 82% of
14 participating hospital information security leaders reported having a significant security

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

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

²¹ Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET, March 3, 2010,
<https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/> (last
visited October 28, 2020).

²² *Id.*

1 incident within the last 12 months, with a majority of these known incidents being caused
2 by “bad actors” such as cybercriminals.²³ “Hospitals have emerged as a primary target
3 because they sit on a gold mine of sensitive personally identifiable information for
4 thousands of patients at any given time. From Social Security Numbers and insurance
5 policies to next of kin and credit cards, no other organization, including credit bureaus,
6 have so much monetizable information stored in their data centers.”²⁴

7 64. Indeed, the *HIPAA Journal* 2019 Healthcare Data Breach Report
8 demonstrates an upward trend in health sector data breaches over the past 10 years, with
9 2019 reflecting more data breaches than any other year.²⁵ 2019 represented a 37.4%
10 increase over breaches reported in 2018 with a total number of patient records exposed
11 increasing from 13,947,909 in 2018 to 41,335,889.²⁶ “Shockingly, the report disclosed
12 that in 2019 alone, the healthcare records of 12.55% of the population of the United States
13 were exposed, impermissibly disclosed, or stolen.”²⁷

14 65. As a healthcare services provider, Magellan knew, or certainly should have
15 known, the importance of safeguarding patient PHI and PII entrusted to it and of the
16 foreseeable consequences if its data security systems were breached, including the

17 ²³ HIMSS, 2019 *HIMSS Cybersecurity Survey*, [https://www.himss.org/himss-](https://www.himss.org/himss-cybersecurity-survey)
18 [cybersecurity-survey](https://www.himss.org/himss-cybersecurity-survey) (last visited October 28, 2020).

19 ²⁴ Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*,
20 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)
21 [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).

22 ²⁵ *Healthcare Data Breach Statistics*, HIPAA Journal, [https://www.hipaajournal.](https://www.hipaajournal.com/health-care-data-breach-statistics/)
23 [com/health](https://www.hipaajournal.com/health-care-data-breach-statistics/)
[care-data-breach-statistics/](https://www.hipaajournal.com/health-care-data-breach-statistics/) (last visited October 28, 2020).

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

27 ²⁷ *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 significant costs that would be imposed on its employees, providers, and patients as a
2 result of a breach. But Magellan failed to take adequate cybersecurity measures to
3 prevent the Data Breach from occurring.

4 ***F. Magellan Acquires, Collects, and Stores Plaintiffs' and Class Members' PII and***
5 ***PHI***

6 66. As its Privacy Policy makes clear, Magellan Health acquires, collects, and
7 stores a massive amount of PII on its employees, former employees, and beneficiaries.

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

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

15 69. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and
16 Class Members' PII and PHI, Magellan assumed legal and equitable duties and knew or
17 should have known that it was responsible for protecting Plaintiffs' and Class Members'
18 PII and PHI from unauthorized disclosure.

19 70. At all times relevant hereto, Plaintiffs and Class Members took reasonable
20 steps to maintain the confidentiality of their PII and PHI. Plaintiffs and Class Members
21 relied on Magellan to keep their PII and PHI confidential and securely maintained, to use
22 this information for business purposes only, and to make only authorized disclosures of
23 this information.

24 ***G. The Value of Personally Identifiable Information and the Effects of***
25 ***Unauthorized Disclosure***

26 71. Personally identifiable information is a valuable commodity to identity
27 thieves. As the FTC recognizes, identity thieves can use it to commit an array of crimes
28

1 including identify theft, medical and financial fraud.²⁸ Indeed, a robust “cyber black
2 market” exists in which criminals openly post stolen PII on multiple underground Internet
3 websites.

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

9 73. For example, the Social Security Administration has warned that identity
10 thieves can use an individual’s Social Security Number to apply for additional credit
11 lines. Such fraud may go undetected until debt collection calls commence months, or
12 even years, later. Stolen Social Security Numbers also make it possible for thieves to file
13 fraudulent tax returns, file for unemployment benefits, or apply for a job using a false
14 identity. Each of these fraudulent activities is difficult to detect. An individual may not
15 know that his or her Social Security Number was used to file for unemployment benefits
16 until law enforcement notifies the individual’s employer of the suspected fraud.
17 Fraudulent tax returns are typically discovered only when an individual’s authentic tax
18 return is rejected.

19 74. Moreover, it is not an easy task to change or cancel a stolen Social Security
20 Number. An individual cannot obtain a new Social Security Number without significant
21 paperwork and evidence of actual misuse. Even then, a new Social Security Number may
22 not be effective, as “[t]he credit bureaus and banks are able to link the new number very
23 quickly to the old number, so all of that old bad information is quickly inherited into the
24 new Social Security number.”²⁹

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

27 ²⁹ *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR, Brian
28 Naylor, Feb. 9, 2015, <http://www.npr.org/2015/02/09/384875839/data-stolen-by->

1 75. This data, as one would expect, demands a much higher price on the black
2 market. Martin Walter, senior director at cybersecurity firm RedSeal, explained,
3 “[c]ompared to credit card information, personally identifiable information and Social
4 Security Numbers are worth more than 10x on the black market.”³⁰ As explained above,
5 the inclusion of PHI, such as the information exposed here, is even more valuable.

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

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

11 77. The Federal Trade Commission (“FTC”) has promulgated numerous
12 guides for businesses which highlight the importance of implementing reasonable data
13 security practices. According to the FTC, the need for data security should be factored
14 into all business decision-making.³¹

15 78. In 2016, the FTC updated its publication, *Protecting Personal Information:
16 A Guide for Business*, which established cybersecurity guidelines for businesses.³² The
17 guidelines note that businesses should protect the personal customer information that they
18 keep; properly dispose of personal information that is no longer needed; encrypt

19 _____
20 anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited October 28,
2020).

21 ³⁰ *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*,
22 IT World, Tim Greene, Feb. 6, 2015, [http://www.itworld.com/article/2880960/anthem-
23 hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html](http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html) (last
visited October 28, 2020).

24 ³¹ Federal Trade Commission, *Start with Security*,
25 [https://www.ftc.gov/system/files/documents/plain-language/pdf0205-
startwithsecurity.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf) (last visited October 28, 2020).

26 ³² 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).

1 information stored on computer networks; understand their network’s vulnerabilities; and
2 implement policies to correct any security problems.

3 79. The FTC further recommends that companies not maintain PHI and PII
4 longer than is needed for authorization of a transaction; limit access to sensitive data;
5 require complex passwords to be used on networks; use industry-tested methods for
6 security; monitor for suspicious activity on the network; and verify that third-party
7 service providers have implemented reasonable security measures.³³

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

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

19 82. Magellan was at all times fully aware of its obligation to protect the PII and
20 PHI of employees, providers and patients because of its position as an employer,
21 contractor and healthcare provider. Magellan was also aware of the significant
22 repercussions that would result from its failure to do so.

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

24 83. Data exfiltrated from healthcare providers continues to be a high value
25 target among cybercriminals. This is true whether the data maintained by providers
26 relates to patients or their providers or their own employees. In 2017, the U.S. healthcare
27 sector experienced over 330 Data Breaches, a number which continued to grow in 2018

28 ³³ FTC, *Start With Security*, *supra* note 27.

1 (363 breaches).³⁴ The costs of healthcare Data Breaches are among the highest across all
2 industries, topping \$380 per stolen record in 2017 as compared to the global average of
3 \$141 per record.³⁵ As a result, both the government and private sector have developed
4 industry best standards to address this growing problem.

5 84. The Department of Health and Human Services' Office for Civil Rights
6 ("HHS") notes that "[w]hile all organizations need to implement policies, procedures,
7 and technical solutions to make it harder for hackers to gain access to their systems and
8 data, this is especially important in the healthcare industry. Hackers are actively targeting
9 healthcare organizations as they store large quantities of highly sensitive and valuable
10 data."³⁶ HHS highlights several basic cybersecurity safeguards that can be implemented
11 to improve cyber resilience which require a relatively small financial investment, yet can
12 have a major impact on an organization's cybersecurity posture including: (a) the proper
13 encryption of PHI and PII; (b) educating and training healthcare employees on how to
14 protect PHI and PII; and (c) correcting the configuration of software and network devices.

15 85. Private cybersecurity firms have also identified the healthcare sector as
16 being particularly vulnerable to cyberattacks, both because of the value of the
17 individuals' PHI and PII they maintain and because as an industry they have been slow
18 to adapt and respond to cybersecurity threats.³⁷ They too have promulgated similar best
19

20
21 ³⁴ Identity Theft Resource Center, *2018 End of Year Data Brach Report*,
22 https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf (last visited October 28, 2020).

23 ³⁵ *Id.*

24 ³⁶ *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).

26 ³⁷ *See, e.g.*, <https://resources.infosecinstitute.com/category/healthcare-information-security/is-best-practices-for-healthcare/10-best-practices-for-healthcare-security/#gref>
27 (last visited October 28, 2020).
28

1 practices for bolstering cybersecurity and protecting against the unauthorized disclosure
2 of PHI and PII.

3 86. Despite the abundance and availability of information regarding
4 cybersecurity best practices for the healthcare industry, Magellan chose to ignore them.
5 These best practices were known, or should have been known by Magellan, whose failure
6 to heed and properly implement them directly led to the Data Breach and the unlawful
7 exposure of PII and PHI for a second time.

8
9
10
11 ***J. Defendant Should Have Implemented Appropriate Security Measures***

12 87. As explained by the Federal Bureau of Investigation, “[p]revention is the
13 most effective defense against ransomware and it is critical to take precautions for
14 protection.”³⁸

15 88. To prevent and detect ransomware attacks, including the ransomware
16 attack that resulted in the Data Breach, Defendant could and should have implemented,
17 as recommended by the United States Government, the following measures:

- 18
19
20
21
22
23
24
25
26
- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
 - Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
 - Scan all incoming and outgoing emails to detect threats and filter executable

27 ³⁸ See How to Protect Your Networks from RANSOMWARE, at 3, available at
28 <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view> (last visited Mar. 15, 2021).

1 files from reaching end users.

- 2 • Configure firewalls to block access to known malicious IP addresses.
- 3 • Patch operating systems, software, and firmware on devices. Consider using
4 a centralized patch management system.
- 5 • Set anti-virus and anti-malware programs to conduct regular scans
6 automatically.
- 7 • Manage the use of privileged accounts based on the principle of least
8 privilege: no users should be assigned administrative access unless absolutely
9 needed; and those with a need for administrator accounts should only use them
10 when necessary.
- 11 • Configure access controls—including file, directory, and network share
12 permissions—with least privilege in mind. If a user only needs to read specific
13 files, the user should not have write access to those files, directories, or shares.
- 14 • Disable macro scripts from office files transmitted via email. Consider using
15 Office Viewer software to open Microsoft Office files transmitted via email
16 instead of full office suite applications.
- 17 • Implement Software Restriction Policies (SRP) or other controls to prevent
18 programs from executing from common ransomware locations, such as
19 temporary folders supporting popular Internet browsers or
20 compression/decompression programs, including the
21 AppData/LocalAppData folder.
- 22 • Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- 23 • Use application whitelisting, which only allows systems to execute programs
24 known and permitted by security policy.
- 25 • Execute operating system environments or specific programs in a virtualized
26 environment.
- 27 • Categorize data based on organizational value and implement physical and
28 logical separation of networks and data for different organizational units.³⁹

89. To prevent and detect ransomware attacks, including the ransomware
attack that resulted in the Data Breach, Defendant could and should have implemented,

³⁹ *Id.* at 3-4.

1 as recommended by the United States Cybersecurity & Infrastructure Security Agency,
2 the following measures:

- 3 • **Update and patch your computer.** Ensure your applications and operating
4 systems (OSs) have been updated with the latest patches. Vulnerable
5 applications and OSs are the target of most ransomware attacks....
- 6 • **Use caution with links and when entering website addresses.** Be careful
7 when clicking directly on links in emails, even if the sender appears to be
8 someone you know. Attempt to independently verify website addresses (e.g.,
9 contact your organization's helpdesk, search the internet for the sender
10 organization's website or the topic mentioned in the email). Pay attention to
11 the website addresses you click on, as well as those you enter yourself.
12 Malicious website addresses often appear almost identical to legitimate sites,
13 often using a slight variation in spelling or a different domain (e.g., .com
14 instead of .net)....
- 15 • **Open email attachments with caution.** Be wary of opening email
16 attachments, even from senders you think you know, particularly when
17 attachments are compressed files or ZIP files.
- 18 • **Keep your personal information safe.** Check a website's security to ensure
19 the information you submit is encrypted before you provide it....
- 20 • **Verify email senders.** If you are unsure whether or not an email is legitimate,
21 try to verify the email's legitimacy by contacting the sender directly. Do not
22 click on any links in the email. If possible, use a previous (legitimate) email
23 to ensure the contact information you have for the sender is authentic before
24 you contact them.
- 25 • **Inform yourself.** Keep yourself informed about recent cybersecurity threats
26 and up to date on ransomware techniques. You can find information about
27 known phishing attacks on the Anti-Phishing Working Group website. You
28 may also want to sign up for CISA product notifications, which will alert you
when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been
published.
- **Use and maintain preventative software programs.** Install antivirus
software, firewalls, and email filters—and keep them updated—to reduce
malicious network traffic....⁴⁰

⁴⁰ See Security Tip (ST19-001) Protecting Against Ransomware (original release date
Apr. 11, 2019), available at <https://us-cert.cisa.gov/ncas/tips/ST19-001> (last visited Mar.
15, 2021).

1 90. To prevent and detect ransomware attacks, including the ransomware
2 attack that resulted in the Data Breach, Defendant could and should have implemented,
3 as recommended by the Microsoft Threat Protection Intelligence Team, the following
4 measures:

5 **Secure internet-facing assets**

- 6 - Apply latest security updates
7 - Use threat and vulnerability management
8 - Perform regular audit; remove privileged credentials;

9 **Thoroughly investigate and remediate alerts**

- 10 - Prioritize and treat commodity malware infections as potential full
11 compromise;

12 **Include IT Pros in security discussions**

- 13 - Ensure collaboration among [security operations], [security
14 admins], and [information technology] admins to configure servers
and other endpoints securely;

15 **Build credential hygiene**

- 16 - Use [multifactor authentication] or [network level authentication]
17 and use strong, randomized, just-in-time local admin passwords

18 **Apply principle of least-privilege**

- 19 - Monitor for adversarial activities
20 - Hunt for brute force attempts
21 - Monitor for cleanup of Event Logs
22 - Analyze logon events

23 **Harden infrastructure**

- 24 - Use Windows Defender Firewall
25 - Enable tamper protection
26 - Enable cloud-delivered protection
27 - Turn on attack surface reduction rules and [Antimalware Scan
28

Interface] for Office [Visual Basic for Applications].⁴¹

1
2
3 91. In addition to failing to monitor ingress and ingress network traffic;
4 maintain an inventory of public facing Ips; monitor elevated privileges; equip its server
5 with anti-virus or anti-malware; and employ basic file integrity monitoring, the
6 occurrence of the Data Breach indicates that Defendant failed to adequately implement
7 one or more of the above measures to prevent ransomware attacks, resulting in the Data
8 Breach and the exposure of the PII of approximately X individuals, including Plaintiff
9 and Class Members.

10 92. According to the University of Illinois Chicago (UIC), “To improve
11 cybersecurity in health care, organizations need to hire informatics professionals who can
12 not only collect, manage and leverage data, but protect it as well.”⁴²

13 93. UIC has identified several strategies and best practices that, at a minimum,
14 should be implemented by healthcare providers like Defendant, including but not limited
15 to: establishing a security culture; protecting mobile devices; thoroughly educating all
16 employees; strong passwords that need to be changed regularly; multi-layer security,
17 including firewalls, anti-virus, and anti-malware software; limit network access; control
18 physical access to devices; encryption, making data unreadable without a password or
19 key; multi-factor authentication; backup data, and; limiting employees access to sensitive
20 and protected data.⁴³

21
22
23 ⁴¹ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020),
24 available at <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/> (last visited Mar. 15, 2021).

25 ⁴² See *Cybersecurity: How Can It Be Improved in Health Care?*, Health Informatics-
26 University of Illinois Chicago (last viewed: Dec. 9, 2020),
<https://healthinformatics.uic.edu/blog/cybersecurity-how-can-it-be-improved-in-health-care/>.

27 ⁴³ *Id.*
28

1 94. A number of industry and national best practices have been published and
2 should be used as a go-to resource when developing an institution's cybersecurity
3 standards. The Center for Internet Security (CIS) released its Critical Security Controls,
4 and all healthcare institutions are strongly advised to follow these actions.⁴⁴

5 95. Other best cybersecurity practices that are standard in the healthcare
6 industry include installing appropriate malware detection software; monitoring and
7 limiting the network ports; protecting web browsers and email management systems;
8 setting up network systems such as firewalls, switches and routers; monitoring and
9 protection of physical security systems; protection against any possible communication
10 system; training staff regarding critical points.

11 96. Upon information and belief, Defendant failed to meet the minimum
12 standards of the following cybersecurity frameworks: the NIST Cybersecurity
13 Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4,
14 PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3,
15 DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet
16 Security's Critical Security Controls (CIS CSC), which are established standards in
17 reasonable cybersecurity readiness.

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

19 97. 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 such information and damage to victims may continue for years. Consumer victims of
22 Data Breaches are more likely to become victims of identity fraud.⁴⁵

23 98. The PII and PHI belonging to Plaintiffs and Class Members is private,
24 sensitive in nature, and was left inadequately protected by Defendant, who did not obtain

25 _____
26 ⁴⁴ <https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq/> (last accessed
December 10, 2020)

27 ⁴⁵ 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 Plaintiffs' or Class Members' consent to disclose such sensitive information to any other
2 person as required by applicable law and industry standards.

3 99. Plaintiffs and Class Members have suffered actual injuries from having
4 their PII and PHI exposed as a result of the Data Breach, as identified elsewhere, and
5 including, but not limited to: (a) damages resulting from taking the time to: search for
6 fraudulent activity; change banks, bank accounts, and debit and credit cards; purchase
7 credit monitoring and identity theft protection; call their creditors to provide them with
8 notice of the breach; and otherwise attempt to protect their financial accounts; (b)
9 imminent and impending injury arising from the increased risk of fraud and identity theft;
10 and (d) in other ways to be discovered and proven at trial.

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

14 101. The Data Breach was a direct and proximate result of Magellan's failure
15 to: (a) properly safeguard and protect Plaintiffs' and Class Members' PII and PHI from
16 unauthorized access, use, and disclosure, as required by various state and federal
17 regulations, industry practices, and common law; (b) establish and implement appropriate
18 administrative, technical, and physical safeguards to ensure the security and
19 confidentiality of Plaintiffs' and Class Members' PII and PHI; (c) protect against
20 reasonably foreseeable threats to the security or integrity of such information; and (d) do
21 other things to be discovered and proven at trial.

22 102. Defendant had the resources necessary to prevent the Data Breach, but
23 neglected to adequately invest in data security measures, despite its obligations to protect
24 PII and PHI. Had Defendant remedied the deficiencies in its data security systems and
25 adopted security measures recommended by experts in the field, especially given the
26 previous breach, it would have certainly prevented the intrusions into its systems and,
27 ultimately, the theft of PII and PHI here.

28

1 103. As a direct and proximate result of Defendant’s wrongful actions and
2 inactions, Plaintiffs and Class Members have been placed at an imminent, immediate,
3 and continuing increased risk of harm from identity theft and fraud, requiring them to
4 take time away from other life demands such as work and family to mitigate the actual
5 and potential impact of the Data Breach on their lives. The U.S. Department of Justice’s
6 Bureau of Justice Statistics found that “among victims who had personal information
7 used for fraudulent purposes, 29% spent a month or more resolving problems” and that
8 “resolving the problems caused by identity theft [could] take more than a year for some
9 victims.”⁴⁶

10 104. To date, Magellan has offered inadequate identity monitoring services to
11 affected individuals given the type of data stolen. They are wholly inadequate as they
12 fail to provide for the fact that victims of Data Breaches and other unauthorized
13 disclosures commonly face multiple years of ongoing identity theft and financial fraud
14 and they entirely fail to provide any compensation for the unauthorized release and
15 disclosure of Plaintiffs’ and Class Members’ PII and PHI.

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

- 18 a. The compromise, publication, theft, and/or unauthorized use of their
19 PII and PHI;
- 20 b. Out-of-pocket costs associated with the prevention, detection,
21 recovery, and remediation from identity theft or fraud;
- 22 c. Lost opportunity costs and lost wages associated with efforts
23 expended and the loss of productivity from addressing and
24 attempting to mitigate the actual and future consequences of the
25 Data Breach, including but not limited to efforts spent researching

26
27 ⁴⁶ 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 how to prevent, detect, contest, and recover from identity theft and
2 fraud;

3 d. The continued risk to their PII and PHI, which remains in the
4 possession of Defendant and is subject to further breaches so long
5 as Defendant fails to undertake appropriate measures to protect the
6 PII and PHI in its possession; and

7 e. Current and future costs in terms of time, effort, and money that will
8 be expended to prevent, detect, contest, remediate, and repair the
9 impact of the Data Breach for the remainder of the lives of Plaintiffs
10 and Class Members.

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

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

17 108. The United States Government Accountability Office released a report in
18 2007 regarding Data Breaches (“GAO Report”) in which it noted that victims of identity
19 theft will face “substantial costs and time to repair the damage to their good name and
20 credit record.”⁴⁷

21 109. The FTC recommends that identity theft victims take several steps to
22 protect their personal and financial information after a Data Breach, including contacting
23 one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts
24 for 7 years if someone steals their identity), reviewing their credit reports, contacting

25
26 ⁴⁷ 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
27 2007, *2, <https://www.gao.gov/new.items/d07737.pdf> (last visited October 28, 2020)
28 (“GAO Report”).

1 companies to remove fraudulent charges from their accounts, placing a credit freeze on
2 their credit, and correcting their credit reports.⁴⁸

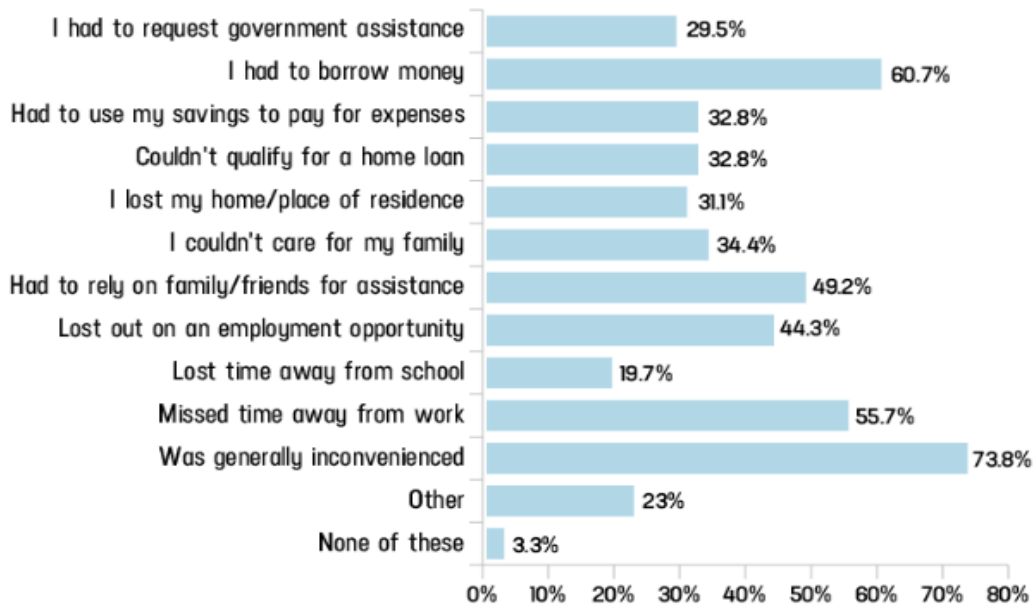
3 110. Identity thieves use stolen personal information such as Social Security
4 Numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and
5 bank/finance fraud.

6 111. Identity thieves can also use Social Security Numbers to, *inter alia*, obtain
7 a driver's license or official identification card in the victim's name but with the thief's
8 picture; use the victim's name and Social Security number to obtain government benefits;
9 or file a fraudulent tax return using the victim's information. In addition, identity thieves
10 may obtain a job using the victim's Social Security number, rent a house or receive
11 medical services in the victim's name, and may even give the victim's personal
12 information to police during an arrest resulting in an arrest warrant being issued in the
13 victim's name. A study by Identity Theft Resource Center shows the multitude of harms
14 caused by fraudulent use of personal and financial information:⁴⁹

15
16
17
18
19
20
21
22
23
24
25
26 ⁴⁸ See <https://www.identitytheft.gov/Steps> (last visited October 28, 2020).

27 ⁴⁹ 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> (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

112. What’s more, PII constitutes a valuable property right, the theft of which is gravely serious.⁵⁰ 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.

113. Theft of PHI, in particular, is gravely serious: “A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your

⁵⁰ 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 insurance provider, or get other care. If the thief’s health information is mixed with yours, your
2 treatment, insurance and payment records, and credit report may be affected.”⁵¹

3 114. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and
4 other healthcare service providers often purchase PII/PHI on the black market for the purpose
5 of target marketing their products and services to the physical maladies of the data breach
6 victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust
7 their insureds’ medical insurance premiums.

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

12 [L]aw enforcement officials told us that in some cases, stolen data
13 may be held for up to a year or more before being used to commit
14 identity theft. Further, once stolen data have been sold or posted on
15 the Web, fraudulent use of that information may continue for years.
16 As a result, studies that attempt to measure the harm resulting from
17 Data Breaches cannot necessarily rule out all future harm.

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

19 116. PII and financial information are such valuable commodities to identity
20 thieves that once the information has been compromised, criminals often trade the
21 information on the “cyber black-market” for years.

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

27 ⁵¹ *See* Medical Identity Theft, Federal Trade Commission Consumer Information (last
28 visited: Dec 9, 2020), [http://www.consumer.ftc.gov/articles/0171-medical-identity-
theft](http://www.consumer.ftc.gov/articles/0171-medical-identity-theft).

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

6 119. For example, the Social Security Administration has warned that identity
7 thieves can use an individual's Social Security number to apply for additional credit lines.
8 Such fraud may go undetected until debt collection calls commence months, or even
9 years, later. Stolen Social Security Numbers also make it possible for thieves to file
10 fraudulent tax returns, file for unemployment benefits, or apply for a job using a false
11 identity. Each of these fraudulent activities is difficult to detect. An individual may not
12 know that his or her Social Security Number was used to file for unemployment benefits
13 until law enforcement notifies the individual's employer of the suspected fraud.
14 Fraudulent tax returns are typically discovered only when an individual's authentic tax
15 return is rejected.

16 120. Moreover, it is not an easy task to change or cancel a stolen Social Security
17 number. An individual cannot obtain a new Social Security number without significant
18 paperwork and evidence of actual misuse. Even then, a new Social Security number may
19 not be effective, as "[t]he credit bureaus and banks are able to link the new number very
20 quickly to the old number, so all of that old bad information is quickly inherited into the
21 new Social Security number."⁵²

22 121. This data, as one would expect, demands a much higher price on the black
23 market. Martin Walter, senior director at cybersecurity firm RedSeal, explained,
24

25
26 ⁵² *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Brian
27 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,
28 2020).

1 “[c]ompared to credit card information, personally identifiable information and Social
2 Security Numbers are worth more than 10x on the black market.”⁵³

3 122. Medical information is especially valuable to identity thieves. The asking
4 price on the Dark Web for medical data is \$50 and up.⁵⁴

5 123. Because of its value, the medical industry has experienced
6 disproportionately higher numbers of data theft events than other industries.

7 124. Defendant therefore knew or should have known this risk and strengthened
8 its data systems accordingly. Defendant was put on notice of the substantial and
9 foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

10 **CLASS ACTION ALLEGATIONS**

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

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

17 126. Alternatively, Plaintiffs propose the following definitions for the following
18 subclasses of Class Members (collectively, “Subclasses”);

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

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

25 ⁵³ *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*,
26 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 visited October 28, 2020).

27 ⁵⁴ See Omri Toppol, *Email Security: How You Are Doing It Wrong & Paying Too Much*,
28 LogDog (Feb. 14, 2016), <https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong/> (last accessed December 10, 2020).

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

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

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

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

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

21 128. Plaintiffs hereby reserve the right to amend or modify the Class definition
22 with greater specificity or division after having had an opportunity to conduct discovery.

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

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

 131. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Rule
23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common
questions of law and fact that predominate over any questions affecting individual Class
Members. The common questions include:

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

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

27 **133. Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4),
28 Plaintiffs are adequate representatives of the Class because they are members of the

1 Class they seek to represent; are committed to pursuing this matter against Magellan to
2 obtain relief for the Class; and have no conflicts of interest with the Class. Moreover,
3 Plaintiffs' attorneys are competent and experienced in litigating class actions, including
4 privacy litigation of this kind. Plaintiffs intend to vigorously prosecute this case and will
5 fairly and adequately protect the Class' interests.

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

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

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

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

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

FIRST CAUSE OF ACTION
NEGLIGENCE

(On Behalf of Plaintiffs Culberson, Rayam, Leather, Williams, Ranson, Flanders, and Lewis and their respective Subclasses, and the Nationwide Class)

138. Plaintiffs restate and reallege paragraphs 1 through 137 as if fully set forth herein.

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

1 140. Plaintiffs and all Class Members entrusted their PII and PHI to Magellan
2 Health with the understanding that the Defendant would safeguard their information.

3 141. Magellan Health had full knowledge of the sensitivity of this PII and PHI
4 and the types of harm that Plaintiffs and Class Members could and would suffer if such
5 information was wrongfully disclosed.

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

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

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

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

27 146. Defendant breached its duties, and thus was negligent and/or grossly
28 negligent, by failing to use reasonable measures to protect Class Members’ PII and PHI.

1 The specific negligent acts and omissions committed by Defendant include, but are not
2 limited to, the following:

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

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

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

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

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

25 151. Defendant was able to protect against the harm suffered by Plaintiffs and
26 Class Members as a result of the Data Breach.

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

1 because this was the second data breach perpetrated in this manner against Defendant in
2 less than a year.

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

5 154. In addition to its general negligence or gross negligence as alleged above,
6 Defendant was also negligent *per se*. Pursuant to the Federal Trade Commission Act (15
7 U.S.C. § 45), Defendant had a duty to provide fair and adequate computer systems and
8 data security practices to safeguard Plaintiffs' and Class Members' PII and PHI. Plaintiffs
9 and Class Members are within the class of persons that the FTC Act was intended to
10 protect.

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

16 156. Defendant violated Section 5 of the FTC Act by failing to use reasonable
17 measures to protect employee and patient PII and PHI and not complying with applicable
18 industry standards, as described in detail herein. Defendant's conduct was particularly
19 unreasonable given the nature and amount of PII and PHI it obtained and stored, the
20 foreseeable consequences of a Data Breach including, specifically, the damages that
21 would result to Plaintiffs and Class Members, and the fact that this was the second time
22 in less than a year that Defendant was the target of a data breach perpetrated in this
23 manner.

24 157. Defendant's violation of Section 5 of the FTC Act constitutes negligence
25 *per se* as Defendant's violation of the FTC Act establishes the duty and breach elements
26 of negligence.

27 158. The harm that occurred as a result of the Data Breach is the type of harm
28 the FTC Act was intended to guard against. The FTC has pursued enforcement actions

1 against businesses, which, as a result of their failure to employ reasonable data security
2 measures and avoid unfair and deceptive practices, caused the same harm as that suffered
3 by Plaintiffs and the Class.

4 159. 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.

7 160. 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.

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

14 162. 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.

16 163. 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.

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

28

1 165. Plaintiffs and Class Members are entitled to compensatory, consequential,
2 and punitive damages in an amount to be proven at trial.

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

7 **SECOND CAUSE OF ACTION**
8 **UNJUST ENRICHMENT**

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

10 167. Plaintiffs restate and reallege paragraphs 1 through 137 as if fully set forth
11 herein.

12 168. Plaintiffs and Class Members conferred a monetary benefit on Defendant.
13 Part of the premiums that health plan participant Plaintiffs and Class Members paid to
14 Defendant (or that were paid to Defendant on behalf of the health plan participant
15 Plaintiffs and Class Members) were intended to be used by Defendant to fund adequate
16 security of Defendant's computer property and Plaintiffs and Class Members' Private
17 Information and protect Plaintiffs and Class Members' Private Information. Employee
18 Plaintiffs and Class Members conferred the benefit of their labor on Defendant, and part
19 of that benefit conferred was intended to be used by Defendant to fund adequate security
20 of Defendant's computer property and employee Plaintiffs and Class Members' Private
21 Information and protect Plaintiffs and Class Members' Private Information.

22 169. Defendant enriched itself by saving the costs it reasonably should have
23 expended on data security measures to secure Plaintiffs' and Class Members' Personal
24 Information. This includes, for example, the costs of monitoring ingress and ingress
25 network traffic; maintaining an inventory of public facing Ips; monitoring elevated
26 privileges; equipping its server with anti-virus or anti-malware; and employing basic file
27 integrity monitoring. Instead of providing a reasonable level of security that would have
28 prevented the Data Breach, Defendant instead calculated to increase its own profits at the

1 expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security
2 measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and
3 proximate result of Defendant' decision to prioritize its own profits over the requisite
4 security.

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

9 171. Defendant acquired the PII and PHI through inequitable means in that it
10 failed to disclose the inadequate security practices previously alleged.

11 172. If Plaintiffs and Class Members knew that Defendant had not secured their
12 PII and PHI, they would not have agreed to provide their PII and PHI to Defendant
13 Magellan Health.

14 173. Plaintiffs and Class Members have no adequate remedy at law.

15 174. As a direct and proximate result of Defendant's conduct, Plaintiffs and
16 Class Members have suffered and will suffer injury, including but not limited to: (a)
17 actual identity theft; (b) the loss of the opportunity to direct how their PII and PHI are
18 used; (c) the compromise, publication, and/or theft of their PII and PHI; (d) out-of-pocket
19 expenses associated with the prevention, detection, and recovery from identity theft,
20 and/or unauthorized use of their PII and PHI; (e) lost opportunity costs associated with
21 effort expended and the loss of productivity addressing and attempting to mitigate the
22 actual and future consequences of the Data Breach, including but not limited to efforts
23 spent researching how to prevent, detect, contest, and recover from identity theft; (f) the
24 continued risk to their PII and PHI, which remains in Defendant's possession and is
25 subject to further unauthorized disclosures so long as Defendant fails to undertake
26 appropriate and adequate measures to protect PII and PHI in its continued possession;
27 and (g) future costs in terms of time, effort, and money that will be expended to prevent,
28

1 detect, contest, and repair the impact of the PII and PHI compromised as a result of the
2 Data Breach for the remainder of the lives of Plaintiffs and Class Members.

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

6 176. Defendant should be compelled to disgorge into a common fund or
7 constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that it
8 unjustly received from them.

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

13 **THIRD CAUSE OF ACTION**
14 **VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW**
15 **Cal. Bus. & Prof. Code §§ 17200, *et seq.***

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

17 178. Plaintiffs restate and reallege paragraphs 1 through 137 as if fully set forth
18 herein.

19 179. Magellan Health is a "person" as defined by Cal. Bus. & Prof. Code §
20 17201.

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

23 181. Magellan Health's unlawful, unfair acts and deceptive acts and practices
24 include:

- 25 a. Magellan Health failed to implement and maintain reasonable
26 security measures to protect Plaintiff's and California Class
27 Members' PII and PHI from unauthorized disclosure, release, Data
28 Breaches, and theft, which was a direct and proximate cause of the

1 Data Breach. This includes failing to: monitor ingress and ingress
2 network traffic; maintain an inventory of public facing Ips; monitor
3 elevated privileges; equip its server with anti-virus or anti-malware;
4 and employ basic file integrity monitoring.;

5 b. Magellan Health failed to identify foreseeable security risks,
6 remediate identified security risks, and adequately improve security
7 following at least one previous cybersecurity incident within the last
8 year. This conduct, with little if any utility, is unfair when weighed
9 against the harm to Plaintiff and California Class Members whose
10 PII and PHI has been compromised;

11 c. Magellan Health's failure to implement and maintain reasonable
12 security measures also was contrary to legislatively declared public
13 policy that seeks to protect consumer data and ensure that entities
14 that are trusted with it use appropriate security measures. These
15 policies are reflected in laws, including the FTC Act, 15 U.S.C. §
16 45, California's Consumer Records Act, Cal. Civ. Code §§
17 1798.81.5 *et seq.*, and California's Consumer Privacy Act, Cal. Civ.
18 Code §§ 1798.100 *et seq.*;

19 d. Magellan Health's failure to implement and maintain reasonable
20 security measures also lead to substantial injuries, as described
21 above, that are not outweighed by any countervailing benefits to
22 consumers or competition. Moreover, because Plaintiff and
23 California Class Members could not know of Magellan Health's
24 inadequate security, consumers could not have reasonably avoided
25 the harms that Magellan Health caused;

26 e. Misrepresenting that it would protect the privacy and confidentiality
27 of Plaintiff's and the California Class Members' PII, including by
28 implementing and maintaining reasonable security measures;

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

20 182. Magellan Health representations and omissions to Plaintiff and California
21 Class Members, which were disseminated to them in California via the patient Notice of
22 Privacy Practices, were material because they were likely to deceive reasonable
23 consumers about the adequacy of Magellan Health's data security and ability to protect
24 the confidentiality of consumers' PII and PHI.

25 183. Magellan Health intended to mislead Plaintiff and the California Class
26 Members and induce them to rely on its misrepresentations and omissions.

27 184. Had Magellan Health disclosed to Plaintiff and the California Class
28 Members that its data systems were not secure and, thus, vulnerable to attack, Magellan

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

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

14 186. As a direct and proximate result of Magellan Health's unfair, unlawful, and
15 fraudulent acts and practices, Plaintiff and California Class Members have suffered and
16 will continue to suffer injury, ascertainable losses of money or property, and monetary
17 and non-monetary damages as described herein and as will be proved at trial.

18 187. Plaintiff and California Class Members seek all monetary and non-
19 monetary relief allowed by law, including restitution of all profits stemming from
20 Magellan Health's unfair, unlawful, and fraudulent business practices or use of their PII;
21 declaratory relief; injunctive relief; reasonable attorneys' fees and costs under California
22 Code of Civil Procedure § 1021.5; and other appropriate equitable relief.

23 188. Plaintiff and California Class Members are also entitled to injunctive relief
24 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 California Class
27 Members.

28 **FOURTH CAUSE OF ACTION**

**VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT,
CAL. CIV. CODE §§ 1798.100, et seq. (§ 1798.150(a))**

(On Behalf of Plaintiff Ranson and the California Subclass)

1
2
3
4 189. Plaintiff restates and realleges paragraphs 1 through 137 as if fully set forth
5 herein.

6 190. Magellan Health is a “business” as defined by Cal. Civ. Code
7 § 1798.140(c).

8 191. Plaintiff Ranson and California Class Members are “consumers” as defined
9 by Cal. Civ. Code § 1798.140(g).

10 192. Plaintiff Ranson’s and California Class Members’ PII and PHI constitutes
11 “personal information” as defined by Cal. Civ. Code § 1798.81.5(d)(1)(A).

12 193. Defendant “collects” consumers’ PII and PHI, including the PHI and PII of
13 Plaintiff Ranson and California Class Members, as defined by Cal. Civ. Code §
14 1798.140(e).

15 194. Defendant violated section 1798.150(a) of the California Consumer
16 Privacy Act (“CCPA”) by failing to prevent Plaintiff Ranson’s and California Class
17 Members’ nonencrypted and nonredacted PII and PHI from unauthorized access and
18 exfiltration, theft, or disclosure as a result of Defendant’s violations of its duty to
19 implement and maintain reasonable security procedures and practices appropriate to the
20 nature of the information to protect the PII and PHI.

21 195. The fact that this was the second data breach in less than a year perpetrated
22 against Defendant in the same way, and that the healthcare industry has been a target of
23 countless data breaches in recent history, as discussed above, indicate that Defendant
24 knew or should have known its security systems, procedures, and practices were
25 inadequate and unreasonable, as do the other facts set forth herein, including that:
26 Defendant failed to monitor ingress and ingress network traffic; failed to maintain an
27 inventory of public facing Ips; failed to monitor elevated privileges; failed to equip its
28

1 server with anti-virus or anti-malware; and failed to employ basic file integrity
2 monitoring.

3 196. As a direct and proximate result of Defendant's violation of its duty,
4 Plaintiff Ranson's and California Class Members' PII and PHI was subjected to an
5 unauthorized access and exfiltration, theft, or disclosure.

6 197. As a direct and proximate result of Magellan Health's violation of its duty,
7 Plaintiff Ranson and California Class Members were injured and lost money or property
8 as described herein and as will be proved at trial.

9 198. Magellan Health knew or should have known that its computer systems and
10 data security practices were inadequate to safeguard Plaintiff Ranson's and California
11 Class Members' PHI and PII entrusted to it, and that risk of a data breach or theft was
12 highly likely.

13 199. Pursuant to section 1798.150(b) of the CCPA, Plaintiff Ranson gave
14 written notice to Magellan Health of its violations of section 1798.150(a). Magellan
15 Health failed to "actually cure" its violations and provide "an express written statement
16 that the violations have been cured and that no further violations shall occur" within 30
17 days of Plaintiff's written notice. Thus, Plaintiff Ranson seeks statutory damages on a
18 class-wide basis.

19 200. Plaintiff Ranson and California Class Members also seek relief under
20 § 1798.150(a), including, but not limited to injunctive or declaratory relief; any other
21 relief the Court deems proper; and attorneys' fees and costs pursuant to Cal. Code Civ.
22 Proc. § 1021.5.

23
24 201. (c) continue to provide adequate credit monitoring to all Missouri Class
25 Members.

26 **FIFTH CAUSE OF ACTION**
27 **VIOLATION OF NEW YORK**
28 **GENERAL BUSINESS LAW § 349**

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

1
2 202. Plaintiffs restate and reallege paragraphs 1 through 137 as if fully set forth
3 herein.

4 203. As detailed above, Defendant represents to patients like Plaintiff Leather
5 that it “has historically held the privacy of patient information as a key tenet of our
6 operations and processes,” and that it has “always implemented policies and procedures
7 for confidentiality that met or exceeded existing state and federal regulations.”⁵⁵

8 204. When Plaintiff Leather became a patient/member of a Magellan Health
9 plan, she was provided with a HIPAA Notice of Privacy Practices (which is a different
10 privacy policy than the one quoted at Paragraph 52 *supra*) that (upon information and
11 belief) promised her that Defendant would: (A) protect the privacy patients’ health
12 information; (B) maintain the privacy of patients’ PHI; (C) use or disclose patients’
13 Protected Health Information (PHI) only for very specific reasons; (D) give patients
14 notice of Defendant’s legal duties and privacy practices with respect to medical
15 information about its patients; (E) follow the terms of the Privacy Notice that is currently
16 in effect; and; (F) not to make any disclosures of PHI without written permission, other
17 than those specifically enumerated in the notice.

18 205. In addition, Defendant represents to patients like Plaintiff Leather that its
19 Security Department “has the task of ensuring that members’ health information is
20 protected as it rests in our systems and when it is exchanged via electronic means,” and
21 that it monitors its computer networks “interfaces to identify inappropriate or
22 unauthorized traffic, e-mail, and attempts to connect to our system.”⁵⁶

23 206. Defendant’s misrepresentations were disseminated in New York via the
24 patient Notice of Privacy Practices.
25

26 ⁵⁵ <https://www.magellanhealth.com/about/compliance/hipaa/> (last visited October 11,
27 2021)

28 ⁵⁶ <https://www.magellanhealth.com/about/compliance/hipaa/> (last visited October 11,
2021)

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

- 4 a. Defendant misrepresented material facts to Plaintiff Leather and the
5 New York Subclass by representing that it would maintain adequate
6 data privacy and security practices and procedures to safeguard
7 Plaintiff and New York Class Members' PHI and PII from
8 unauthorized disclosure, release, Data Breaches, and theft;
- 9 b. Defendant misrepresented material facts to Plaintiff Leather and the
10 New York Subclass by representing that it did and would comply
11 with or exceed the requirements of federal and state laws pertaining
12 to the privacy and security of New York Subclass Members' PHI
13 and PII;
- 14 c. Defendant omitted, suppressed and concealed material facts of the
15 inadequacy of its privacy and security protections for Plaintiff
16 Leather's and New York Subclass Members' PHI and PII;
- 17 d. Defendant engaged in deceptive, unfair, and unlawful trade acts or
18 practices by failing to maintain the privacy and security of Plaintiff
19 Leather's and New York Subclass Members' PHI and PII, in
20 violation of duties imposed by and public policies reflected in
21 applicable federal and state laws, resulting in the Data Breach. These
22 unfair acts and practices violated duties imposed by laws including
23 the Federal Trade Commission Act (15 U.S.C. § 45); and
- 24 e. Defendant engaged in deceptive, unfair, and unlawful trade acts or
25 practices by failing to disclose the Data Breach to Plaintiff Leather
26 and the New York Subclass in a timely and accurate manner,
27 contrary to the duties imposed by N.Y. Gen. Bus. Law § 899-aa(2).
28 At all times relevant herein, Plaintiff Leather and members of the

1 New York Subclass were residents of the State of New York and
2 were deceived in New York by the misconduct alleged herein.

3 208. Defendant knew or should have known that its computer systems and data
4 security practices were inadequate to safeguard Plaintiff Leather's and the New York
5 Subclass Members' PHI and PII entrusted to it, and that risk of a Data Breach or theft
6 was highly likely.

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

9 210. Defendant's failure constitutes false and misleading representations, which
10 have the capacity, tendency, and effect of deceiving or misleading consumers (including
11 Plaintiff Leather and New York Subclass Members) regarding the security of Magellan
12 Health's network and aggregation of PHI and PII.

13 211. The representations upon which consumers (including Plaintiff Leather and
14 New York Subclass Members) relied were material representations (*e.g.*, as to
15 Defendant's adequate protection of PHI and PII), and consumers (including Plaintiff
16 Leather and New York Class Members) relied on those representations to their detriment.

17 212. Defendant's conduct is unconscionable, deceptive, and unfair, as it is likely
18 to, and did, mislead consumers acting reasonably under the circumstances. As a direct
19 and proximate result of Defendant's conduct, Plaintiff Leather and other New York
20 Subclass Members have been harmed, in that they were not timely notified of the Data
21 Breach, which resulted in profound vulnerability to their personal information and other
22 financial accounts.

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

1 b. Representing that its goods and services were of a particular standard or
2 quality when they were of another standard or quality (73 Pa. Stat. § 201-
3 2(4)(vii));

4 c. Advertising its goods and services with intent not to sell them as advertised
5 (73 Pa. Stat. § 201-2(4)(ix); and

6 d. “Engaging in any other ... deceptive conduct which creates a likelihood of
7 confusion or of misunderstanding” (73 Pa. Stat. § 201-2(4)(xxi)).

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

10 222. Magellan Health’s unfair or deceptive acts and practices include but are not
11 limited to: failing to implement and maintain reasonable data security measures to protect
12 Plaintiff’s and Pennsylvania Class Members’ PII and PHI (including failing to: monitor
13 ingress and ingress network traffic; maintain an inventory of public facing Ips; monitor
14 elevated privileges; equip its server with anti-virus or anti-malware; and employ basic
15 file integrity monitoring); failing to identify foreseeable data security risks and remediate
16 the identified risks; failing to comply with common law duties, industry standards
17 including FTC guidance regarding data security; misrepresenting in its Privacy Policy
18 that it would protect Plaintiff’s and Pennsylvania Class Members’ PII and PHI from
19 unauthorized disclosure; and omitting and concealing the material fact that it did not have
20 reasonable measures in place to safeguard such data from thieves stealing it.

21 223. Magellan Health’s representations and omissions were material because
22 they were likely to deceive reasonable consumers including Plaintiff and Pennsylvania
23 Class Members about the adequacy of Magellan Health’s data security practices and
24 ability to protect their PII and PHI.

25 224. Magellan Health intended to mislead Plaintiff and Pennsylvania Class
26 Members and induce them to rely on its misrepresentations and omissions. Plaintiff and
27 Pennsylvania Class Members did rely on Magellan Health’s misrepresentations and
28 omissions relating to its data privacy and security.

1 232. Defendant Magellan Health is a “person, firm, corporation or association”
2 within the meaning of Wis. Stat. § 100.18(1).

3 233. Plaintiff and Wisconsin Class Members are members of “the public”
4 within the meaning of Wis. Stat. § 100.18(1).

5 234. Plaintiff and Wisconsin Class Members were deceived as described herein
6 and have suffered damages as a result of Magellan’s unfair and deceptive trade practices,
7 as complained of herein.

8 235. In addition, Magellan Health operating in Wisconsin, willfully failed to
9 disclose and did actively conceal its inadequate computer and data security discussed
10 herein and otherwise engaged in activities with a tendency or capacity to deceive. This
11 inadequate security includes that Defendant failed to monitor ingress and ingress network
12 traffic; failed to maintain an inventory of public facing Ips; failed to monitor elevated
13 privileges; failed to equip its server with anti-virus or anti-malware; and failed to employ
14 basic file integrity monitoring.

15 236. By failing to disclose that its computer and data systems were inadequately
16 secured and that it lacked sufficiently robust cyber-security protocols, Magellan Health
17 engaged in deceptive business practices in violation of Wis. Stat. § 100.18.

18 237. Magellan Health’s unfair or deceptive acts or practices were likely to and
19 did in fact deceive reasonable consumers, including Plaintiff and Wisconsin
20 Class Members, about the true nature of its computer and data security and the quality of
21 the Magellan Health brand.

22 238. Magellan Health intentionally and knowingly misrepresented material facts
23 regarding the security and integrity of its data systems cyber-security protocols with an
24 intent to mislead Plaintiff and Wisconsin Class Members. Defendant’s
25 misrepresentations were disseminated in Wisconsin via the patient Notice of Privacy
26 Practices.

27 239. Magellan Health knew or should have known that its conduct violated Wis.
28 Stat. § 100.18.

1 240. As alleged above, Magellan Health made material statements about its
2 cyber-security protocols, the integrity of its data systems, and the maintenance of PII that
3 were either false or misleading.

4 241. Magellan Health owed Plaintiff and Wisconsin Class Members a duty to
5 disclose the true nature of the security of its computer and data systems and robustness
6 of its cyber-security protocols and practices because Magellan Health:

- 7 a. Possessed exclusive knowledge regarding the lack of security of its
8 employees' PII;
- 9 b. Intentionally concealed the foregoing from Plaintiff and Wisconsin
10 Class Members; and/or
- 11 c. Made incomplete representations about the security and integrity of
12 its computer and data systems and cyber-security practices.

13 242. Magellan Health's fraudulent claims of computer and data security and the
14 true nature of the security of such systems were material to Plaintiff and Wisconsin
15 Class Members.

16 243. Plaintiff and Wisconsin Class Members suffered ascertainable loss caused
17 by Magellan Health's misrepresentations and its concealment of and failure to disclose
18 material information. Wisconsin Class Members would not have had their PII
19 compromised and would have taken steps to prevent identity theft and other harms, but
20 for Magellan Health's violations described herein.

21 244. Magellan Health had an ongoing duty to all Magellan Health's employees
22 – past and present – as well as members who received benefits from any one of the health
23 plans that is administered, to refrain from unfair and deceptive practices under Wis. Stat.
24 § 100.18.

25 245. All Wisconsin Class Members suffered ascertainable loss, including in the
26 form of out of pocket expenses and lost time to implement and maintain credit freezes
27 and identity theft prevention as a result of Magellan Health's deceptive and unfair acts
28 and practices made in the course of its business.

1 246. Magellan Health’s violations present a continuing risk to Plaintiff
2 and Wisconsin Class Members as well as to the general public.

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

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

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

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

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

17
18
19 **EIGHTH CAUSE OF ACTION**
20 **VIOLATIONS OF THE OF THE FLORIDA UNFAIR AND DECEPTIVE**
21 **TRADE PRACTICES ACT, FLA. STAT. §§ 501.201, *et seq.***

22 *(On Behalf of Plaintiff Lewis and the Florida Subclass)*

23 252. Plaintiffs restate and reallege paragraphs 1 through 137 as if fully set forth
24 herein.

25 253. Plaintiff Lewis and Florida Subclass members are “consumer[s]” as
26 defined by Fla. Stat. § 501.203.

27 254. Defendant engaged in the conduct alleged in this Complaint, and
28 advertised, offered, or sold goods or services in Florida and engaged in trade or commerce

1 directly or indirectly affecting the people of Florida, including Plaintiff Lewis and Florida
2 Class Members.

3 255. Defendant engaged in deceptive, unfair, and unlawful trade acts or
4 practices in the conduct of trade or commerce, in violation of Fla. Stat. § 501.204(1),
5 including but not limited to the following:

- 6 a. failure to maintain adequate computer systems and data security practices
7 to safeguard patient PII and/or PHI, including failing to: monitor ingress
8 and ingress network traffic; maintain an inventory of public facing Ips;
9 monitor elevated privileges; equip its server with anti-virus or anti-
10 malware; and employ basic file integrity monitoring);
- 11 b. failure to disclose that its computer systems and data security practices
12 were inadequate to safeguard patient PII and/or PHI from theft;
- 13 c. failure to timely and accurately disclose the Data Breach to Plaintiff and
14 Florida Class members;
- 15 d. continued acceptance and storage of patient PII and/or PHI after Defendant
16 knew or should have known of the security vulnerabilities of its network
17 that were exploited in the Data Breach; and,
- 18 e. continued acceptance and storage of patient PII and/or PHI after Defendant
19 knew or should have known of the Data Breach and before it allegedly
20 remediated the Data Breach.

21 256. These unfair acts and practices violated duties imposed by laws, including
22 by not limited to the FTCA and Fla. Stat. § 501.171(2).

23 257. Defendant's misrepresentations were disseminated in Florida via the
24 patient Notice of Privacy Practices.

25 258. As a direct and proximate result of Defendant's violation of the Florida
26 Unfair and Deceptive Trade Practices Act, Plaintiff and Florida Class members suffered
27 damages including, but not limited to damages from lost time and effort to mitigate the
28 actual and potential impact of the Data Breach on their lives including, *inter alia*, by

1 overpaying for the products and services sold by Defendant; closely reviewing and
2 monitoring their medical transactions for unauthorized activity, filing police reports, and
3 damages from identity theft, which may take months if not years to discover and detect,
4 given the far-reaching, adverse and detrimental consequences of identity theft and loss of
5 privacy. The nature of other forms of economic damage and injury may take years to
6 detect, and the potential scope can only be assessed after a thorough investigation of the
7 facts and events surrounding the theft mentioned above.

8 259. Also, as a direct result of Defendant's knowing violation of the Florida
9 Unfair and Deceptive Trade Practices Act, Plaintiff Lewis and Florida Class members
10 are entitled to damages as well as injunctive relief, including, but not limited to:

- 11 a. Ordering that Defendant engage third-party security auditors/penetration
12 testers as well as internal security personnel to conduct testing, including
13 simulated attacks, penetration tests, and audits on Defendant's systems on
14 a periodic basis, and ordering Defendants to promptly correct any problems
15 or issues detected by such third-party security auditors;
- 16 b. Ordering that Defendant engage third-party security auditors and internal
17 personnel to run automated security monitoring;
- 18 c. Ordering that Defendant audit, test, and train its security personnel
19 regarding any new or modified procedures;
- 20 d. Ordering that Defendant segment customer data by, among other things,
21 creating firewalls and access controls so that if one area of Defendant's
22 system is compromised, hackers cannot gain access to other portions of
23 Defendant's system;
- 24 e. Ordering that Defendant purge, delete, and destroy patient PII and/or PHI
25 not necessary for its provisions of services in a reasonably secure manner;
- 26 f. Ordering that Defendant conduct regular database scans and security
27 checks;

1 g. Ordering that Defendant routinely and continually conduct internal training
2 and education to inform internal security personnel how to identify and
3 contain a breach when it occurs and what to do in response to a breach; and

4 h. Ordering Defendant to meaningfully educate its customers about the threats
5 they face as a result of the loss of their financial and personal information
6 to third parties, as well as the steps Defendant's customers should take to
7 protect themselves.

8 260. Plaintiff brings this action on behalf of himself and Florida Class Members
9 for the relief requested above and for the public benefit in order to promote the public
10 interests in the provision of truthful, fair information to allow consumers to make
11 informed purchasing decisions and to protect Plaintiff, Florida Class Members and the
12 public from Defendant's unfair methods of competition and unfair, deceptive, fraudulent,
13 unconscionable and unlawful practices. Defendant's wrongful conduct as alleged in this
14 Complaint has had widespread impact on the public at large.

15 261. The above unfair and deceptive practices and acts by Defendant were
16 immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury
17 to Plaintiff Lewis and Florida Class Members that they could not reasonably avoid; this
18 substantial injury outweighed any benefits to consumers or to competition.

19 262. Defendant knew or should have known that its computer systems and data
20 security practices were inadequate to safeguard Florida Class Members' PII and/or PHI
21 and that the risk of a data breach or theft was high.

22 263. Defendant's actions and inactions in engaging in the unfair practices and
23 deceptive acts described herein were negligent, knowing and willful, and/or wanton and
24 reckless.

25 264. Plaintiff and Florida Class Members seek relief under the Florida Deceptive
26 and Unfair Trade Practices Act, Fla. Stat. §§ 501.201, *et seq*, including, but not limited
27 to, damages, restitution, injunctive relief, and/or attorney fees and costs, and any other
28 just and proper relief.

PRAYER FOR RELIEF

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

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

DEMAND FOR JURY TRIAL

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

1 Dated: October 12, 2021

Respectfully submitted,

2
3 **BONNETT, FAIRBOURN,
FRIEDMAN & BALINT, P.C.**

4 By: s/Carrie A. Laliberte

5 Elaine A. Ryan (AZ Bar #012870)
6 Carrie A. Laliberte (AZ Bar #032556)
7 2325 E. Camelback Rd., Suite 300
8 Phoenix AZ 85016
9 Telephone: (602) 274-1100
Email: eryl@bffb.com
claliberte@bffb.com

10
11 **BONNETT, FAIRBOURN,
FRIEDMAN & BALINT, P.C.**

12 Patricia N. Syverson (AZ Bar #020191)
13 9655 Granite Ridge Drive, Suite 200
14 San Diego, California 92123
15 Telephone: (619) 798-4593
Email: psyverson@bffb.com

16 **ZIMMERMAN REED LLP**

17 Hart L. Robinovitch (AZ SBN 020910)
18 14646 North Kierland Blvd., Suite 145
19 Scottsdale, AZ 85254
20 Telephone: (480) 348-6400
Facsimile: (480) 348-6415
Email: hart.robinovitch@zimmreed.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

**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

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

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

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*

CERTIFICATE OF SERVICE

I hereby certify that on October 12, 2021, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will send notice of such filing to all registered users.

/s/ Carrie A. Laliberte
Carrie A. Laliberte

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

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



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:

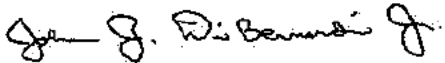
- Ensure that you enroll by: August 31, 2020 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your activation code: [REDACTED]

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.

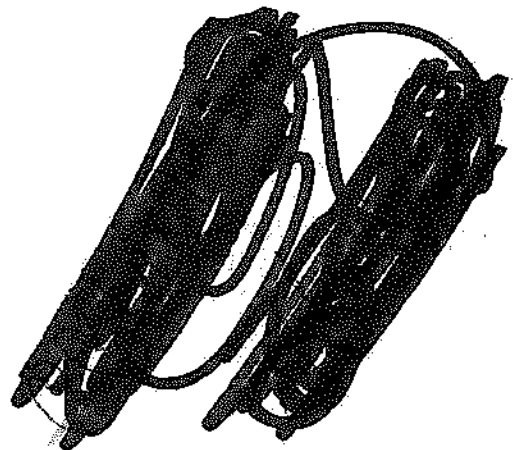
You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

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 current 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 Fair 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

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/identity-theft) to get recovery steps and to file an identity theft complaint. Your complaint will be added to the FTC's Consumer Sentinel Network, where it will be accessible to law enforcers for their investigations.

Should I contact the IRS?

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

- If you received an [IRS 5071C](#) or an [IRS 5747C](#) letter; call the number provided in the notice or, if instructed, visit the IRS's Identity Verification Service at https://go.magellanhealth.com/e/703943/ud-scams-identity-verification/hbglz/100020545?h=ziA8fPKAtJXJjxjkKcGqn62ScaQZf_nN85sloy9fJyl.
- 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



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

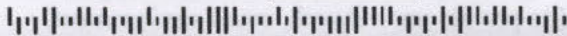
June 26, 2020



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



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]

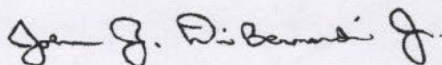
If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 888-451-6558 by September 30, 2020. Be prepared to provide engagement number DB20851 as proof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

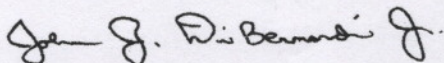
If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 888-451-6558 by September 30, 2020. Be prepared to provide engagement number DB20851 as proof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



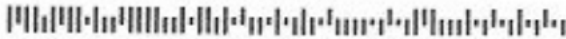
Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

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:

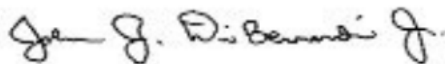
- Ensure that you enroll by: October 31, 2020 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your activation code: [REDACTED]

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

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



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

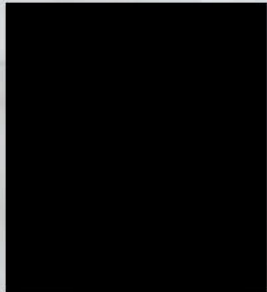
May 15, 2020



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.



Case 2:20-cv-01282-MTL Document 40-6 Filed 10/12/21 Page 3 of 5
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:

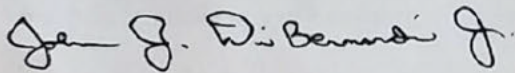
- Ensure that you enroll by: August 31, 2020 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your activation code: [REDACTED]

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/hbg/z/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.

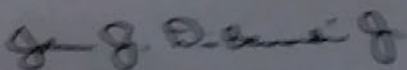
In addition, please be on the lookout for any scams that attempt to lure you into providing personal information in connection with this incident. Magellan will NOT call you or send you any email messages asking for your personal information or credit card information, or send you any email messages 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.



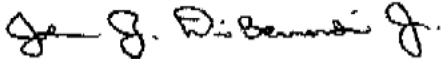
What You Can Do

- 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

EXHIBIT

July 24, 2020

F8631-L04-0033618 P003 T00082 *****ALL FOR AADC 342

KEITH LEWIS

BRADENTON, FL 34207-3314



Dear Keith Lewis:

Magellan Health Inc.¹ ("Magellan"), which provides services to **The Health Benefits Plan of 7-Eleven Inc.**, 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

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

www.magellanhealth.com

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.

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.

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 any of your 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: 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]

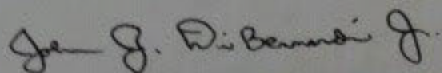
If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 888-451-6558 by October 31, 2020. Be prepared to provide engagement number DB21423 as proof of 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