Jean S. Martin (admitted *pro hac vice*)
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Fax: (813) 223-5402
jeanmartin@forthepeople.com

Bryan L. Bleichner (admitted *pro hac vice*)
Philip J. Krzeski (admitted *pro hac vice)*
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Telephone: (612) 339-7300
Fax: (612) 336-2940
bbleichner@chestnutcambronne.com
pkrzeski@chestnutcambronne.com

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Dillan Clarke, Elayne Martinez, Brian Kircher, Juanita Sarabia, Megan Kircher, Donald Banti and Marcia Banti, Ryan Mangum and Tiffany Mangum, Anthony Spano, Carol Ashby, Margaret O'Grady, Mayra Esquival and her minor son, E. N., on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

Yuma Regional Medical Center,

Defendant.

Case No. 2:22:cv-01061-PHX-SMB

PLAINTIFFS' FIRST AMENDED CONSOLIDATED CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiffs Dillan Clarke, Elayne Martinez, Brian Kircher, Juanita Sarabia, Megan Kircher, Donald Banti and Marcia Banti, Ryan Mangum and Tiffany Mangum, Anthony Spano, Carol Ashby, Margaret O'Grady, Mayra Esquival and her minor son, E.N. ("Plaintiffs") bring this Amended Consolidated Class Action Complaint against Defendant Yuma Regional Medical Center ("YRMC" or "Defendant")—and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities—on behalf of themselves and all others similarly situated, and allege as follows:

NATURE OF THE ACTION

1. This class action arises from YRMC's failure to properly secure and safeguard Plaintiffs' and 700,000 Class Members' highly sensitive protected health information ("PHI")[1] and personally identifiable information ("PII")[2] (collectively, "Private Information"). As a result, Plaintiffs' and the Class's Private Information was **stolen** from YRMC's systems during a massive and preventable data breach and is now in

[1] The Department of Health and Human Services ("HHS") defines "protected health information" as "individually identifiable health information . . . that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium." 45 C.F.R. § 160.103. "Health information" means "any information, including genetic information, whether oral or recorded in any form or medium, that: (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual." *Id.*

[2] The Federal Trade Commission ("FTC") defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth. . . ..." 17 C.F.R. § 248.201(b)(8).

the hands of cybercriminals who target Private Information for its value in committing fraud and identity theft.

2. On April 25, 2022, YRMC detected a ransomware attack after the attack caused a disruption to its network. After an investigation, YRMC learned that cybercriminals gained access to its systems between April 21, 2022, and April 25, 2022, and, prior to encrypting files on YRMC's network, **stole** a subset of files from YRMC's systems (the "Data Breach" or "Breach"). Within these stolen files contained the confidential Private Information of Plaintiffs and the Class, including their Social Security numbers.

3. Despite discovering the Breach on April 25, 2022, YRMC waited over two (2) months to notify victims that their highly sensitive PII and PHI was ***stolen*** by cybercriminals during the Data Breach. This delay in notice exacerbated Plaintiffs' and Class Members' damages by depriving Plaintiffs and Class Members of crucial time to mitigate and address the Data Breach in a timely manner, including by placing credit freezes on their accounts or obtaining identity theft protection services.

4. When Defendant finally notified victims of the Data Breach, it deliberately underplayed the severity of the Data Breach. Defendant's Notice of Data Breach Letters ("Notice Letter") failed to confirm how many people were impacted, how the Breach occurred, or account for the delay in notifying impacted patients. To date, these critical facts have not been provided to Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information is protected.

5. On information and belief, Defendant's systems were accessible to cybercriminals because Defendant failed to implement and/or maintain reasonable security measures to protect its patients' Private Information, leaving it an easy target for theft and

misuse. Defendant admits as much in its Notice Letter, stating "[t]o help prevent something like this from happening again, we strengthened the security of our systems and will continue enhancing our protocols to safeguard the information in our care."

6. The Data Breach—which Defendant failed to detect until cybercriminals had already ***copied and stolen*** Plaintiffs' and Class Members' Private Information—is the direct result of Defendant's failure to implement basic data security measures. Had Defendant implemented reasonable cybersecurity measures—including adequate safeguards for initial access, encryption, redaction of personal data elements, and sufficient logging, monitoring, and alerting tools to detect unauthorized activity—the cybercriminals would not have been able to hack into Defendant's systems and exfiltrate Plaintiffs' and the Class's Private Information before being detected.

7. By failing to detect the Data Breach and timely notify victims, Defendant violated Arizona law, industry standards, and duties of care, leaving Plaintiffs and Class Members vulnerable to identity theft without adequate warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their Private Information.

8. Defendant offered Plaintiffs temporary, non-automatic credit monitoring and identity theft protection services. Such abbreviated and non-automatic credit and identity protection is insufficient protection for those impacted by the Data Breach as their Private Information was taken by unknown cybercriminals and can be used for fraudulent means at any time in the future. Defendant's offering of abbreviated, non-automatic monitoring will not prevent the unauthorized use of its patients' Private Information but will only alert patients after misuse has already occurred.

9. Unfortunately, the risk of identity theft caused by this Data Breach has materialized. Plaintiffs' and Class Members' Private Information was targeted, accessed,

and stolen by cybercriminals. The *modus operandi* of cybercriminals involves stealing Private Information for financial gain. Indeed, hackers targeted and stole Plaintiffs' and Class Members' Private Information from Defendant because of the data's value in exploiting and stealing Plaintiffs' and Class Members' identities. The present and continuing risk to Plaintiffs and Class Members as victims of the Data Breach will remain for their respective lifetimes.

10. Defendant knew or should have known Plaintiffs and putative Class Members deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of their unencrypted, Private Information being accessed on Defendant's network by an unauthorized third party.

11. Defendant's misconduct has injured the Plaintiffs and members of the proposed Class, including: (i) the lost or diminished value of their Private Information; (ii) costs associated with the prevention, detection, and recovery from identity theft, tax fraud, and other unauthorized use of their data; (iii) lost opportunity costs to mitigate the Data Breach's consequences, including lost time; (iv) lost time value of money that was stolen or unavailable due to the Data Breach; (v) invasion of their privacy; and (vi) emotional distress associated with the loss of control over their highly sensitive Private Information.

12. Plaintiffs and Class Members are victims of Defendant's negligence and inadequate cybersecurity practices. Plaintiffs and Class Members trusted Defendant with their Private Information. But Defendant betrayed that trust. Defendant failed to use up-to-date security practices to prevent the Data Breach. None of this should have happened because the Data Breach was entirely preventable.

13. Plaintiffs and Class Members seek compensatory, nominal, statutory, and punitive damages, declaratory judgment, and injunctive relief to redress the wide spread damages caused by Defendant's Data Breach.

PARTIES

14. Plaintiff **Dillan Clarke** is a resident and citizen of Arizona, residing in Yuma. Plaintiff Clarke received a Notice Letter dated June 9, 2022, from Defendant stating that unauthorized actors gained access to files on Yuma's network. The compromised files contained Plaintiff Clarke's Private Information.

15. Plaintiff **Elayne Martinez** is a resident and citizen of Arizona, residing in Yuma. Plaintiff Martinez received a Notice Letter dated June 9, 2022, from Defendant stating that unauthorized actors gained access to files on Yuma's network. The compromised files contained Plaintiff Martinez's Private Information.

16. Plaintiff **Brian Kircher** is a resident and citizen of Arizona, residing in Phoenix. Plaintiff Kircher received a Notice Letter dated June 9, 2022, from Defendant stating that unauthorized actors gained access to files on Yuma's network. The compromised files contained Plaintiff Brian Kircher's Private Information.

17. Plaintiff **Megan Kircher** is a natural person and citizen of Arizona, residing in Yuma, Arizona. Plaintiff M. Kircher received a Notice Letter dated June 9, 2022, from Defendant stating that unauthorized actors gained access to files on Yuma's network. The compromised files contained Plaintiff Megan Kircher's Private Information.

18. Plaintiff **Juanita Sarabia** is a natural person and citizen of Arizona, residing in Yuma, Arizona. Plaintiff Sarabia received a Notice Letter dated June 9, 2022, from Defendant YRMC stating that unauthorized actors gained access to files on Yuma's network. The compromised files contained Plaintiff Sarabia's Private Information.

19. Plaintiffs **Donald and Marcia Banti** ("Banti Plaintiffs") are residents and citizens of Arizona, residing in Yuma, Arizona. The Banti Plaintiffs received notice that unauthorized actors gained access to files on Yuma's network. The compromised files contained the Banti Plaintiffs' Private Information.

20. Plaintiffs **Ryan and Tiffany Mangum** ("Mangum Plaintiffs") are residents and citizens of Arizona, residing in Yuma, Arizona. The Mangum Plaintiffs received a Notice Letter dated June 9, 2022, from Defendant stating that unauthorized actors gained access to files on Yuma's network. The compromised files contained the Mangum Plaintiffs' Private Information.

21. Plaintiff **Anthony Spano** is a natural person and citizen of Arizona, residing in Yuma, Arizona. Plaintiff Spano received a Notice Letter dated June 9, 2022, from Defendant stating that unauthorized actors gained access to files on Yuma's network. The compromised files contained Plaintiff Spano's Private Information.

22. Plaintiff **Carol Ashby** is a natural person and citizen of Arizona, residing in Yuma, Arizona. Plaintiff Ashby received a Notice Letter from Defendant stating that unauthorized actors gained access to files on Yuma's network. The compromised files contained Plaintiff Ashby's Private Information.

23. Plaintiff **Margaret O'Grady** is a natural person and citizen of Arizona, residing in Yuma, Arizona. Plaintiff O'Grady received a Notice Letter from Defendant stating that unauthorized actors gained access to files on Yuma's network. The compromised files contained Plaintiff O'Grady's Private Information.

24. Plaintiff **Mayra Esquival** and her minor son, E.N., are residents and citizens of Arizona, residing in Yuma, Arizona. Plaintiff Esquival received a Notice Letter from

Defendant stating that unauthorized actors gained access to files on Yuma's network. The compromised files contained Plaintiffs Mayra Esquival's and E.N.'s Private Information.

25. Defendant **Yuma Regional Medical Center** is a 406-bed hospital established in 1964. Defendant is an Arizona corporation with its principal place of business at 2400 South Avenue A, Yuma, Arizona, in Yuma County, 85364.

JURISDICTION AND VENUE

26. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity.

27. This Court has personal jurisdiction over Defendant because Defendant is headquartered in Arizona and conducts substantial business in this District. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant is headquartered in this District, and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

FACTUAL ALLEGATIONS

A. Defendant's Failure to Safeguard Patients' Private Information

28. Plaintiffs and Class Members are Defendant's current and former patients. As a condition of receiving medical treatment, Defendant requires its patients to provide their Private Information.

29. On information and belief, in its ordinary course of business, Defendant maintains records of its past and current patients' information, including its patients' full names, Social Security numbers, financial account information, credit-card information,

dates of birth, prescription information, diagnosis information, treatment information, treatment providers, health insurance information, medical information, and Medicare/Medicaid ID numbers, in the ordinary course of business. These records are stored on Defendant's computer systems.

30. When Defendant collects this sensitive information from its patients, it promises to employ reasonable measures to safeguard the Private Information from theft and misuse.

31. Defendant states in its Notice of Privacy Practices ("NOPP") that it is "committed to protecting the confidentiality of [its patients'] medical information …."[3] Upon information and belief, this NOPP (or one with similar language) was provided to Plaintiffs and Class Members when they received medical services, and Plaintiffs and Class Members were required to provide written acknowledgment that they received the NOPP.

32. Defendant's Privacy Policy further states that patients should "expect that treatment records are confidential unless you have given permission to release information or reporting is required or permitted by law."[4]

33. Defendant, through its actions and statements, represented that its patients' Private Information would be secure. These representations were underscored by the fact that Plaintiffs and Class Members recognized the confidential nature of their medical information and Defendant's duty, as a medical provider, to employ protections. Plaintiffs and Class Members relied on these representations when agreeing to provide their Private

---

[3] *Notice of Privacy Practices*, YUMA REGIONAL MEDICAL CENTER, https://www.onvidahealth.org//wp-content/uploads/2023/12/NoticePrivacyPractices English-Mobile-App-Language-Added-122823-FINAL.pdf (last visited Dec. 8, 2024).

[4] *Patient Rights and Responsibilities*, ONVIDA HEALTH, https://www.onvidahealth.org/patients-and-visitors/your-hospital-stay/patient-rights-and-responsibilities/ (last visited Dec. 8, 2024).

Information to Defendant in order to receive medical care and treatment.

34. Despite its alleged commitments to securing sensitive patient data, Defendant ***does not*** follow industry standard practices in securing patients' Private Information.

35. In April 2022, hackers bypassed Defendant's inadequate security safeguards and infiltrated its systems, giving them unfettered access to patients' Private Information. The Data Breach occurred because threat actors "took advantage of security holes within hospital networks[.]"[5] Other reports note that "[a]lthough the Yuma Regional Medical Center (YMRC) took its systems offline briefly after detecting the incident, threat actors were still able to extract critical files from the compromised servers."[6]

36. Experts in the cybersecurity field have commented on the Data Breach. Specifically, Gary Ogasawara, the CTO of Cloudian, noted that "[t]he exposure of patient data at Yuma Regional Medical Center again highlights why organizations need to encrypt sensitive data (both in flight and at rest) to protect against ransomware attacks."[7]

37. Upon information and belief, Defendant did not have adequate cybersecurity employees on staff at the time of the Data Breach. In a May 2024 podcast, Defendant's VP and CISO, Blaine Hebert, discussed that he has "been there approximately a year now[]" and described the hospital as having a "[p]retty small cyber team[]" with "four direct

---

[5] *See Next-Gen Healthcare Data Breach Incidents and Solutions*, PUREWL, https://www.purewl.com/next-gen-healthcare-data-breach-incidents-and-solutions/ (last visited Dec. 12, 2024).

[6] *See* Vlad Constantinescu, *700,000 Social Security Numbers Leaked in Attack on Major Arizona Hospital*, BITDEFENDER (June 14, 2022), https://www.bitdefender.com/en-us/blog/hotforsecurity/700-000-social-security-numbers-leaked-in-attack-on-major-arizona-hospital (last visited Dec. 1, 2024).

[7] Tim Sandle, *Yuma Regional Medical Center Hit by Cyberattack*, DIGITAL JOURNAL (July 9, 2022) https://www.digitaljournal.com/tech-science/yuma-regional-medical-center-hit-by-cyberattack/article (last visited Dec. 12, 2024).

reports that fall underneath [him]." Critically, Hebert admitted that he is "*the first CISO that Yuma Regional has had*. Prior to that, they had some virtual CISOs that were supporting the organization." (emphasis added).[8]

38. These characterizations of the Data Breach and Defendant's cybersecurity measures suggest gaps, and—upon information and belief—inadequacies regarding Defendant's security systems and networks storing patient information, including the failure to encrypt patient information.

39. Upon information and belief, and pursuant to Defendant's own limited admissions, the unauthorized individuals had unfettered access to patients' Private Information from April 21, 2022, to April 25, 2022, and removed files from Defendant's systems.

40. In response to the Data Breach, Defendant contends that it "strengthened the security of [its] systems and will continue enhancing [its] protocols to safeguard the information in [its] care." This is insufficient, particularly for Plaintiffs and Class Members, as these additional measures should have been in place ***before*** the Data Breach.

41. Defendant's Notice Letter, as well as its website notice, both omit the size and scope of the Data Breach. Defendant has demonstrated a pattern of providing inadequate notices and disclosures about the Data Breach.

42. On information and belief, Defendant does not adequately train its employees on cybersecurity policies, enforce those policies, or maintain reasonable security practices and systems.

---

[8] Anthony Guerra, *Q&A with Yuma Regional Medical Center VP/CISO, Blaine Hebert: Getting the Basics Right Goes a Long Way*, HEALTHSYSTEMCIO.COM (May 8, 2024), https://healthsystemcio.com/2024/05/08/yuma-regional-medical-ciso-blaine-hebert/ (last visited Dec. 12, 2024).

43. Defendant's negligent conduct caused the Data Breach. Defendant violated its obligation to implement best practices and comply with industry standards concerning computer system security. Defendant failed to comply with security standards and allowed its patients' Private Information to be accessed and stolen by failing to implement security measures that could have prevented, mitigated, or timely detected the Data Breach.

44. Though Defendant offered victims temporary, non-automatic credit monitoring and identity theft protection services in its Notice Letter, these remedies are inadequate. Because of Plaintiffs' and Class Members' increased risk of future harm, they will need to use these services indefinitely.

45. Once unencrypted Private Information is taken by unauthorized individuals, the Private Information can end up anywhere, be bought by anyone, and be used at any time in the future. Given the lifelong harm that the Data Breach poses to Defendant's former and current patients, the offering of these temporary monitoring services do not adequately address the harm its patients have suffered and will continue to suffer for many years to come.

B. Plaintiffs' Experiences

i. Plaintiff Dillan Clarke

46. Plaintiff Clarke is a former patient who received medical services from Defendant. Plaintiff Clarke provided Defendant with monetary compensation in exchange for medical services. Defendant also required Plaintiff to provide it with her Private Information so that it could perform services and collect payment. Plaintiff Clarke intended that a portion of the price she paid Defendant for services would be used to provide adequate data security. Defendant understood that Plaintiff Clarke had this expectation, as evidenced by the statements in its NOPP and the sensitivity of the data it possessed.

47. Plaintiff Clarke entrusted Defendant with her Private Information with the shared understanding that her information would be adequately protected from foreseeable threats. This shared understanding is evidenced from the Notice of Privacy Practices that she was provided and reviewed when receiving care. This shared understanding is further evidenced by the Privacy Policy on Defendant's website.

48. Upon information and belief, Plaintiff Clarke's Private Information was stored on Defendant's network during the Data Breach and presently remains in Defendant's possession.

49. Defendant sent Plaintiff a Notice Letter dated June 9, 2022, stating that its network was accessed by unauthorized third parties and indicating that Plaintiff's Private Information was stolen during this event.

50. Plaintiff Clarke is very careful about sharing her sensitive Private Information. Plaintiff Clarke has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Clarke stores any documents containing her Private Information in a safe and secure location or destroys the documents.

51. Plaintiff Clarke suffered an intangible privacy injury from the theft of her Private Information and its subsequent disclosure to third parties for criminal purposes. Plaintiff Clarke's loss of privacy and the substantial risk of imminent harm Plaintiff now faces has caused Plaintiff Clarke to suffer proportionate fear and anxiety.

52. As a result of the Data Breach, Plaintiff Clarke has spent hours dealing with the consequences of the Data Breach to mitigate and minimize her damages. This includes verifying the legitimacy of the notice of the Data Breach, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. Plaintiff Clarke's time

spent on these matters is not only reasonable, but necessary; her failure to do so could result in her missing fraudulent activity and result in greater damages than what she has already incurred. This time has been lost forever and cannot be recaptured. Even the Notice Letter that Defendant sent Plaintiff about the Data Breach encouraged her to spend time mitigating the present and increased risk of harm.

53. Plaintiff Clarke has suffered actual injury in the form of damages to and diminution in the value of her Private Information—a form of intangible property that Plaintiff Clarke entrusted to Defendant, which was compromised as a result of the Data Breach.

54. Plaintiff Clarke has also experienced actual injury in the form of identity theft. After the Data Breach, Plaintiff Clarke had her personal debit card compromised, leaving her unable to use the funds in her debit card and checking account for days. Plaintiff learned of this fraud after her bank contacted her to ask if she attempted to access her account through a new device. As a result of this fraudulent activity, Plaintiff suffered injury from the lost time value of the funds in this account. Plaintiff lost time communicating with her bank about this fraud and suffered anxiety and emotional distress proportionate to the substantially increased risk of harm that she now faces, which is evidenced by this fraudulent activity.

55. Shortly after the Data Breach, Plaintiff Clarke experienced a significant increase in the receipt of spam e-mail messages, phone calls, and text messages because of the Data Breach. Upon information and belief, this was because of the Data Breach, particularly given the timing and fact that much of the spam was medical related.

56. As a result of the Data Breach, Plaintiff faces a substantial risk of imminent harm that will remain the rest of her life. Plaintiff also faces a substantial risk of harm from

a future Data Breach because her information remains, upon information and belief, inadequately protected in Defendant's possession. Plaintiff Clarke has a continuing interest in ensuring that her Private Information is protected from foreseeable future threats.

ii. Plaintiff Elayne Martinez

57. Plaintiff Martinez is a current patient of Defendant. Plaintiff Martinez provided Defendant with monetary compensation in exchange for medical services. Defendant also required Plaintiff Martinez to provide it with her Private Information so that it could perform services and collect payment. Plaintiff Martinez intended that a portion of the price she paid Defendant for services would be used to provide adequate data security. Defendant understood that Plaintiff Martinez had this expectation, as evidenced by the statements in its NOPP and the sensitivity of the data it possessed.

58. Plaintiff Martinez entrusted Defendant with her Private Information with the shared understanding that her information would be adequately protected from foreseeable threats. This shared understanding is evidenced from the Notice of Privacy Practices that she was provided and reviewed when receiving care. This shared understanding is further evidenced by the Privacy Policy on Defendant's website.

59. Upon information and belief, Plaintiff Martinez's Private Information was stored on Defendant's network during the Data Breach and presently remains in Defendant's possession.

60. Defendant sent Plaintiff a Notice Letter dated June 9, 2022, stating that its network was accessed by unauthorized third parties and indicating that Plaintiff's Private Information was stolen during this event.

61. Plaintiff Martinez is very careful about sharing her sensitive Private Information. Plaintiff has never knowingly transmitted unencrypted sensitive Private

Information over the internet or any other unsecured source. Plaintiff Martinez stores any documents containing her Private Information in a safe and secure location or destroys the documents.

62. Plaintiff Martinez suffered an intangible privacy injury from the theft of her Private Information and its subsequent disclosure to third parties for criminal purposes. Plaintiff Martinez's loss of privacy and the substantial risk of imminent harm Plaintiff now faces has caused Plaintiff Martinez to suffer proportionate fear and anxiety.

63. As a result of the Data Breach, Plaintiff Martinez has spent hours dealing with the consequences of the Data Breach to mitigate and minimize her damages. This includes verifying the legitimacy of the notice of the Data Breach, exploring credit monitoring and identity theft protection services, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. Plaintiff time spent on these matters is not only reasonable, but necessary; her failure to do so could result in her missing fraudulent activity and result in greater damages than she has already incurred. This time has been lost forever and cannot be recaptured. Even the Notice Letter that Defendant sent Plaintiff about the Data Breach encouraged her to spend time mitigating the increased risk of harm.

64. During the duration of the Data Breach and subsequent network outage, despite trying, Plaintiff was unable to access her medical test results or to schedule appointments with her physicians via Defendant's online systems.

65. Plaintiff Martinez suffered actual injury in the form of damages to and diminution in the value of her Private Information—a form of intangible property that Plaintiff Martinez entrusted to Defendant, which was compromised in and as a result of the Data Breach.

66. Since the Data Breach, Plaintiff has received an increase in spam e-mails, text messages, and phone calls regarding medically related matters. Plaintiff Martinez has received several confirmation emails for medical appointments she did not make, each containing accurate personal information. Upon information and belief, this was because of the Data Breach, particularly given the timing and fact that much of the spam was medical related.

67. After the Data Breach, Plaintiff Martinez was informed that her family members have received several phone calls from persons claiming to be Plaintiff, and that during these calls, the apparent identity thieves.

68. As a result of the Data Breach, Plaintiff Martinez faces a substantial risk of imminent harm that will remain the rest of her life. Plaintiff also faces a substantial risk of harm from a future Data Breach because her information remains, upon information and belief, inadequately protected in Defendant's possession. Plaintiff Martinez has a continuing interest in ensuring that her Private Information is protected from foreseeable future threats.

iii. Plaintiff Brian Kircher

69. Plaintiff Brian Kircher is a current patient of Defendant's. Beginning in approximately 2008, Plaintiff provided Defendant with monetary compensation in exchange for medical services. Defendant also required Plaintiff Brian Kircher to provide it with his Private Information so that it could perform services and collect payment. Plaintiff intended that a portion of the price he paid Defendant for services would be used to provide adequate data security. Defendant understood that Plaintiff Brian Kircher had this expectation, as evidenced by the statements in its NOPP and the sensitivity of the data it possessed.

70. Plaintiff Brian Kircher entrusted Defendant with his Private Information with the shared understanding that his information would be adequately protected from foreseeable threats. This shared understanding is evidenced from the Notice of Privacy Practices that he was provided and reviewed when receiving care. This shared understanding is further evidenced by the Privacy Policy on Defendant's website.

71. Upon information and belief, Plaintiff Brian Kircher's Private Information was stored on Defendant's network during the Data Breach and presently remains in Defendant's possession.

72. Defendant sent Plaintiff Brian Kircher a Notice Letter dated June 9, 2022, stating that its network was accessed by unauthorized third parties and indicating that Plaintiff Brian Kircher's Private Information was stolen during this event.

73. Plaintiff Brian Kircher is very careful about sharing his sensitive Private Information. Plaintiff Brian Kircher has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Brian Kircher stores any documents containing his Private Information in a safe and secure location or destroys the documents.

74. Plaintiff Brian Kircher suffered an intangible privacy injury from the theft of his Private Information and its subsequent disclosure to third parties for criminal purposes. Plaintiff Brian Kircher's loss of privacy and the substantial risk of imminent harm he now faces has caused Plaintiff to suffer proportionate fear and anxiety.

75. As a result of the Data Breach, Plaintiff Brian Kircher has spent more than six (6) hours dealing with the consequences of the Data Breach to mitigate and minimize his damages. This includes verifying the legitimacy of the notice of the Data Breach, exploring credit monitoring and identity theft protection services, and self-monitoring his

accounts and credit reports to ensure no fraudulent activity has occurred. Plaintiff Brian Kircher time spent on these matters is not only reasonable, but necessary; his failure to do so could result in his missing fraudulent activity and result in greater damages than she has already incurred. This time has been lost forever and cannot be recaptured. Even the Notice Letter that Defendant sent Plaintiff Brian Kircher about the Data Breach encouraged him to spend time mitigating the increased risk of harm.

76. Plaintiff Brian Kircher suffered actual injury in the form of damages to and diminution in the value of his Private Information—a form of intangible property that Plaintiff Brian Kircher entrusted to Defendant, which was compromised in and as a result of the Data Breach.

77. As a result of the Data Breach, Plaintiff faces a substantial risk of imminent harm that will remain the rest of his life. Plaintiff Brian Kircher also faces a substantial risk of harm from a future Data Breach because his information remains, upon information and belief, inadequately protected in Defendant's possession. Plaintiff Brian Kircher has a continuing interest in ensuring that his Private Information is protected from foreseeable future threats.

iv. Plaintiff Megan Kircher

78. Plaintiff Megan Kircher is Defendant's current patient. Beginning in approximately 2022, Plaintiff Megan Kircher provided Defendant with monetary compensation in exchange for medical services. Defendant also required Plaintiff Megan Kircher to provide it with her Private Information so that it could perform services and collect payment. Plaintiff Megan Kircher intended that a portion of the price she paid Defendant for services would be used to provide adequate data security. Defendant understood that Plaintiff Megan Kircher had this expectation, as evidenced by the

statements in its NOPP and the sensitivity of the data it possessed.

79. Plaintiff Megan Kircher entrusted Defendant with her Private Information with the shared understanding that her information would be adequately protected from foreseeable threats. This shared understanding is evidenced from the Notice of Privacy Practices that she was provided and reviewed when receiving care. This shared understanding is further evidenced by the Privacy Policy on Defendant's website.

80. Upon information and belief, Plaintiff Megan Kircher's Private Information was stored on Defendant's network during the Data Breach and presently remains in Defendant's possession.

81. Defendant sent Plaintiff Megan Kircher a Notice Letter dated June 20, 2022, stating that its network was accessed by unauthorized third parties and indicating that Plaintiff's Private Information was stolen during this event.

82. Plaintiff Megan Kircher is very careful about sharing her sensitive Private Information. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff stores any documents containing her Private Information in a safe and secure location or destroys the documents.

83. Plaintiff Megan Kircher suffered an intangible privacy injury from the theft of her Private Information and its subsequent disclosure to third parties for criminal purposes. Plaintiff's loss of privacy and the substantial risk of imminent harm she now faces has caused her to suffer proportionate fear and anxiety.

84. As a result of the Data Breach, Plaintiff Megan Kircher has spent more than ten (10) hours dealing with the consequences of the Data Breach to mitigate and minimize his damages. This includes verifying the legitimacy of the notice of the Data Breach, exploring credit monitoring and identity theft protection services, and self-monitoring her

accounts and credit reports to ensure no fraudulent activity has occurred. Plaintiff time spent on these matters is not only reasonable, but necessary; her failure to do so could result in her missing fraudulent activity and result in greater damages than she has already incurred. This time has been lost forever and cannot be recaptured. Even the Notice Letter that Defendant sent Plaintiff about the Data Breach encouraged her to spend time mitigating the increased risk of harm.

85. Plaintiff Megan Kircher suffered actual injury in the form of damages to and diminution in the value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

86. Since the Data Breach, Plaintiff Megan Kircher has also received an increase in spam e-mails, text messages, and phone calls regarding medically related matters.

87. As a result of the Data Breach, Plaintiff Megan Kircher faces a substantial risk of imminent harm that will remain the rest of her life. Plaintiff also faces a substantial risk of harm from a future Data Breach because her information remains, upon information and belief, inadequately protected in Defendant's possession. Plaintiff Megan Kircher has a continuing interest in ensuring that her Private Information is protected from foreseeable future threats.

v. Plaintiff Juanita Sarabia

88. Plaintiff Sarabia is Defendant's current patient. Beginning in approximately 2021, Plaintiff provided Defendant with monetary compensation in exchange for medical services. Defendant also required Plaintiff Sarabia to provide it with her Private Information so that it could perform services and collect payment. Plaintiff Sarabia intended that a portion of the price she paid Defendant for services would be used to

provide adequate data security. Defendant understood that Plaintiff Sarabia had this expectation, as evidenced by the statements in its NOPP and the sensitivity of the data it possessed.

89. Plaintiff Sarabia entrusted Defendant with his Private Information with the shared understanding that her information would be adequately protected from foreseeable threats. This shared understanding is evidenced from the Notice of Privacy Practices that she was provided and reviewed when receiving care. This shared understanding is further evidenced by the Privacy Policy on Defendant's website.

90. Upon information and belief, Plaintiff Private Information was stored on Defendant's network during the Data Breach and presently remains in Defendant's possession.

91. Defendant sent Plaintiff Sarabia a Notice Letter dated June 9, 2022, stating that its network was accessed by unauthorized third parties and indicating that Plaintiff's Private Information was stolen during this event.

92. Plaintiff Sarabia is very careful about sharing her sensitive Private Information. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff stores any documents containing her Private Information in a safe and secure location or destroys the documents.

93. Plaintiff Sarabia suffered an intangible privacy injury from the theft of her Private Information and its subsequent disclosure to third parties for criminal purposes. Plaintiff's loss of privacy and the substantial risk of imminent harm Plaintiff now faces has caused Plaintiff to suffer proportionate fear and anxiety.

94. As a result of the Data Breach, Plaintiff Sarabia has spent more than three (3) hours dealing with the consequences of the Data Breach to mitigate and minimize her

damages. This includes verifying the legitimacy of the notice of the Data Breach, exploring credit monitoring and identity theft protection services, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. Plaintiff time spent on these matters is not only reasonable, but necessary; her failure to do so could result in his missing fraudulent activity and result in greater damages than she has already incurred. This time has been lost forever and cannot be recaptured. Even the Notice Letter that Defendant sent Plaintiff Sarabia about the Data Breach encouraged her to spend time mitigating the increased risk of harm.

95. Plaintiff Sarabia also experienced actual injury in the form of fraud and identity theft. After the Data Breach, in or around August 2022, Plaintiff Sarabia was notified by her credit monitoring service, Credit Karma and her bank that her personal information (including Social Security numbers) was detected on the "dark web."

96. Because of the Data Breach and subsequent dark web notification, in or around August 2022, Plaintiff upgraded free Credit Karma account with a paid credit monitoring subscription for one year. This subscription cost approximately $97.50 for one year. Given that harms like fraudulent activity and identity theft following data breaches often go undetected for months, or even years, Plaintiff Sarabia's purchase of credit monitoring services is a reasonable and necessary step to remain appraised of the risks associated with her information, and remain a necessary mitigation tool for years to come.

97. Plaintiff Sarabia suffered actual injury in the form of damages to and diminution in the value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

98. Since the Data Breach, Plaintiff Sarabia has also received an increase in spam

e-mails, text messages, and phone calls regarding medically related matters.

99. As a result of the Data Breach, Plaintiff Sarabia faces a substantial risk of imminent harm that will remain the rest of her life. Plaintiff also faces a substantial risk of harm from a future Data Breach because her information remains, upon information and belief, inadequately protected in Defendant's possession. Plaintiff Sarabia has a continuing interest in ensuring that her Private Information is protected from foreseeable future threats.

vi. The Banti Plaintiffs

100. Plaintiffs Donald and Marcia Banti are medical patients of Yuma Regional. Beginning in 2022, Plaintiffs provided Defendant with monetary compensation in exchange for medical services. Defendant also requires Plaintiffs to provide it with their Private Information so that Defendant could perform services and collect payment. The Banti Plaintiffs intended that a portion of the price they paid Defendant for services would be used to provide adequate data security. Defendant understood that the Banti Plaintiffs had this expectation, as evidenced by the statements in its NOPP and the sensitivity of the data it possessed.

101. The Banti Plaintiffs entrusted Defendant with their Private Information based on the shared understanding that their information would be adequately protected from foreseeable threats. This shared understanding is evidenced by the Notice of Privacy Practices that they were provided and reviewed when receiving care. This shared understanding is further evidenced by the Privacy Policy on Defendant's website.

102. Upon information and belief, the Banti Plaintiffs' Private Information was stored on Defendant's network during the Data Breach and presently remains in Defendant's possession.

103. Defendant sent the Banti Plaintiffs a Notice Letter dated June 9, 2022, stating

that its network was accessed by unauthorized third parties and indicating that the Banti Plaintiffs' Private Information was stolen during this event.

104. The Banti Plaintiffs are very careful about sharing their sensitive Private Information. The Banti Plaintiffs have never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiffs store any documents containing their Private Information in a safe and secure location or destroy the documents.

105. The Banti Plaintiffs suffered intangible privacy injuries from the theft of their Private Information and its subsequent disclosure to third parties for criminal purposes. The Banti Plaintiffs' loss of privacy and the substantial risk of imminent harm Plaintiffs now face have caused them to suffer proportionate fear and anxiety.

106. As a result of the Data Breach, the Banti Plaintiffs have spent hours dealing with the consequences of the Data Breach to mitigate and minimize their damages. This includes verifying the legitimacy of the notice of the Data Breach, exploring credit monitoring and identity theft protection services, and self-monitoring their accounts and credit reports to ensure no fraudulent activity has occurred. The Banti Plaintiffs' time spent on these matters is not only reasonable, but necessary; their failure to do so could result in their missing fraudulent activity and result in greater damages than they already incurred. This time has been lost forever and cannot be recaptured. Even the Notice Letter that Defendant sent the Banti Plaintiffs about the Data Breach encouraged them to spend time mitigating the increased risk of harm.

107. The Banti Plaintiffs also experienced actual injury in the form of identity theft. After the Data Breach, Plaintiff Donald Banti was contacted by Wells Fargo Bank about fraud on his debit card. Upon information and belief, this was possible because threat

actors used the information stolen in the Data Breach combined with other publicly available information to bypass the security measures on this financial account.

108. As a result of the fraudulent activity on his debit card, Plaintiff Donald Banti lost access to his debit card and the funds in this checking account for several days, causing the Banti Plaintiffs to suffer injury from the lost time value of the funds in this account. The Banti Plaintiffs were also required to spend time and effort dealing with this fraudulent activity, including communicating with Wells Fargo and reviewing financial accounts.

109. After the Data Breach, the Banti Plaintiffs have received an increased amount of phone calls, text messages and/or emails from unknown callers. The Banti Plaintiffs have received phone calls and text messages from unknown callers/senders inquiring about medical equipment, medical devices and/or other medically related matters.

110. The Banti Plaintiffs suffered actual injury in the form of damages to and diminution in the value of their Private Information—a form of intangible property that the Banti Plaintiffs entrusted to Defendant, which was compromised in and as a result of the Data Breach.

111. As a result of the Data Breach, the Banti Plaintiffs face a substantial risk of imminent harm that will remain the rest of their lives. The Banti Plaintiffs also face a substantial risk of harm from a future Data Breach because their information remains, upon information and belief, inadequately protected in Defendant's possession. The Banti Plaintiffs have a continuing interest in ensuring that their Private Information is protected from foreseeable future threats.

vii. The Mangum Plaintiffs

112. Plaintiffs Ryan Mangum and Tiffany Mangum are medical patients of Defendant's. Beginning in 2022, the Mangum Plaintiffs provided Defendant with monetary

compensation in exchange for medical services. Defendant also requires the Mangum Plaintiffs to provide it with their Private Information so that Defendant can perform services and collect payment. The Mangum Plaintiffs intended that a portion of the price they paid Defendant for services would be used to provide adequate data security. Defendant understood that the Mangum Plaintiffs had this expectation, as evidenced by the statements in its NOPP and the sensitivity of the data it possessed.

113. The Mangum Plaintiffs entrusted Defendant with their Private Information based on the shared understanding that their information would be adequately protected from foreseeable threats. This shared understanding is evidenced by the Notice of Privacy Practices that they were provided and reviewed when receiving care. This shared understanding is further evidenced by the Privacy Policy on Defendant's website.

114. Upon information and belief, the Mangum Plaintiffs' Private Information was stored on Defendant's network during the Data Breach and presently remains in Defendant's possession.

115. Defendant sent the Mangum Plaintiffs a Notice Letter dated June 9, 2022, stating that its network was accessed by unauthorized third parties and indicating that the Mangum Plaintiffs' Private Information was stolen during this event.

116. The Mangum Plaintiffs are very careful about sharing their sensitive Private Information. Plaintiffs have never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiffs store any documents containing their Private Information in a safe and secure location or destroy the documents.

117. The Mangum Plaintiffs suffered an intangible privacy injury from the theft of their Private Information and its subsequent disclosure to third parties for criminal purposes. The Mangum Plaintiffs' loss of privacy and the substantial risk of imminent harm

that they now face has caused the Mangum Plaintiffs to suffer proportionate fear and anxiety.

118. As a result of the Data Breach, the Mangum Plaintiffs has spent hours dealing with the consequences of the Data Breach to mitigate and minimize their damages. This includes verifying the legitimacy of the notice of the Data Breach, exploring credit monitoring and identity theft protection services, and self-monitoring their accounts and credit reports to ensure no fraudulent activity has occurred. The Mangum Plaintiffs time spent on these matters is not only reasonable, but necessary; their failure to do so could result in their missing fraudulent activity and result in greater damages than they already incurred. This time has been lost forever and cannot be recaptured. Even the Notice Letter that Defendant sent the Mangum Plaintiffs about the Data Breach encouraged them to spend time mitigating the increased risk of harm.

119. The Mangum Plaintiffs suffered actual injury in the form of damages to and diminution in the value of their Private Information—a form of intangible property that the Mangum entrusted to Defendant, which was compromised in and as a result of the Data Breach.

120. After the Data Breach, the Mangum Plaintiffs were informed by CreditWise and Experian that their personal information was on the "dark web."

121. After the Data Breach, the Mangum Plaintiffs have received an increased amount of spam phone calls, text messages, and/or email messages from individuals unknown to Plaintiffs. Specifically, the Mangum Plaintiffs have received phone calls for relief of fake medical debt. Upon information and belief, this was because of the Data Breach, particularly given the timing and fact that much of the spam was medical related.

122. As a result of the Data Breach, the Mangum Plaintiffs face a substantial risk

of imminent harm that will remain the rest of their lives. The Mangum Plaintiffs also face a substantial risk of harm from a future Data Breach because their information remains, upon information and belief, inadequately protected in Defendant's possession. Plaintiffs have a continuing interest in ensuring that their Private Information is protected from foreseeable future threats.

viii. Plaintiff Anthony Spano

123. Plaintiff Spano has been a patient of Defendant's, and its affiliated healthcare providers, since approximately 2007. During this time, Plaintiff Spano has provided Defendant with monetary compensation in exchange for medical services. Defendant also required Plaintiff Spano to provide it with his Private Information so that it could perform services and collect payment. Plaintiff intended that a portion of the price he paid Defendant for services would be used to provide adequate data security. Defendant understood that Plaintiff had this expectation, as evidenced by the statements in its NOPP and the sensitivity of the data it possessed.

124. Plaintiff Spano entrusted Defendant with his Private Information with the shared understanding that his information would be adequately protected from foreseeable threats. This shared understanding is evidenced from the Notice of Privacy Practices that he was provided and reviewed when receiving care. This shared understanding is further evidenced by the Privacy Policy on Defendant's website.

125. Upon information and belief, Plaintiff Spano's Private Information was stored on Defendant's network during the Data Breach and presently remains in Defendant's possession.

126. Defendant sent Plaintiff Spano a Notice Letter dated June 17, 2022, stating that its network was accessed by unauthorized third parties and indicating that Plaintiff

Spano's Private Information was stolen during this event.

127. Plaintiff Spano is very careful about sharing his sensitive Private Information. Plaintiff Spano has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Spano stores any documents containing his Private Information in a safe and secure location or destroys the documents.

128. Plaintiff Spano suffered an intangible privacy injury from the theft of his Private Information and its subsequent disclosure to third parties for criminal purposes. Plaintiff Spano's loss of privacy and the substantial risk of imminent harm Plaintiff Spano now faces has caused Plaintiff Spano to suffer proportionate fear and anxiety.

129. As a result of the Data Breach, Plaintiff Spano has spent more than 100 hours dealing with the consequences of the Data Breach to mitigate and minimize his damages. This includes verifying the legitimacy of the notice of the Data Breach, exploring credit monitoring and identity theft protection services, self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred, closing accounts that have been subjected to fraud, and filing a police report regarding the identity theft and fraud he experienced. Plaintiff Spano time spent on these matters is not only reasonable, but necessary; his failure to do so could result in missing fraudulent activity and result in greater damages than he has already incurred. This time has been lost forever and cannot be recaptured. Even the Notice Letter that Defendant sent Plaintiff Spano about the Data Breach encouraged him to spend time mitigating the increased risk of harm.

130. The day after receiving notice from Defendant regarding the Data Breach, Plaintiff Spano received notification from Experian that someone attempted to change the mailing address on his bank accounts to an address in Florida (a place he does not live).

131. After the Data Breach, in July 2022, Plaintiff Spano also experienced fraudulent transactions on two of his credit cards. Upon information and belief, the threat actor was able to access these accounts using Private Information stolen from the Data Breach in combination with publicly available information. As a result, Plaintiff Spano's was required to cancel his cards. While waiting for his credit cards to be reissued and the fraudulent charges to be removed from his accounts, Plaintiff Spano was unable to use the credit that he had been extended, causing injury from the lost time value of these funds.

132. After—and because of—the Data Breach, Plaintiff Spano froze his credit with the three major credit bureaus (i.e., Experian, TransUnion, Equifax).

133. Plaintiff Spano suffered actual injury in the form of damages to and diminution in the value of his Private Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

134. Since the Data Breach, Plaintiff Spano has also received an increase in spam e-mails, text messages, and phone calls regarding medically related matters.

135. As a result of the Data Breach, Plaintiff faces a substantial risk of imminent harm that will remain the rest of his life. Plaintiff also faces a substantial risk of harm from a future Data Breach because his information remains, upon information and belief, inadequately protected in Defendant's possession. Plaintiff has a continuing interest in ensuring that his Private Information is protected from foreseeable future threats.

ix. Plaintiff Carol Ashby

136. Plaintiff Ashby is Defendant's current patient since January of 1977. Plaintiff provided Defendant with monetary compensation in exchange for medical services. Defendant also required Plaintiff to provide it with her Private Information so that it could

perform services and collect payment. Plaintiff Ashby intended that a portion of the price she paid Defendant for services would be used to provide adequate data security. Defendant understood that Plaintiff Ashby had this expectation, as evidenced by the statements in its NOPP and the sensitivity of the data it possessed.

137. Plaintiff Ashby entrusted Defendant with her Private Information with the shared understanding that her information would be adequately protected from foreseeable threats. This shared understanding is evidenced from the Notice of Privacy Practices that she was provided and reviewed when receiving care. This shared understanding is further evidenced by the Privacy Policy on Defendant's website.

138. Upon information and belief, Plaintiff Ashby's Private Information was stored on Defendant's network during the Data Breach and presently remains in Defendant's possession.

139. Defendant sent Plaintiff Ashby a Notice Letter dated June 9, 2022, stating that its network was accessed by unauthorized third parties and indicating that Plaintiff Ashby's Private Information was stolen during this event.

140. Plaintiff Ashby is very careful about sharing her sensitive Private Information. Plaintiff Ashby has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Ashby stores any documents containing her Private Information in a safe and secure location or destroys the documents.

141. Plaintiff Ashby suffered an intangible privacy injury from the theft of her Private Information and its subsequent disclosure to third parties for criminal purposes. Plaintiff Ashby's loss of privacy and the substantial risk of imminent harm Plaintiff Ashby now faces has caused Plaintiff Ashby to suffer proportionate fear and anxiety.

142. As a result of the Data Breach, Plaintiff Ashby has spent more than 10 hours dealing with the consequences of the Data Breach to mitigate and minimize her damages. This includes verifying the legitimacy of the notice of the Data Breach, exploring credit monitoring and identity theft protection services, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. Plaintiff Ashby time spent on these matters is not only reasonable, but necessary; her failure to do so could result in her missing fraudulent activity and result in greater damages than she has already incurred. This time has been lost forever and cannot be recaptured. Even the Notice Letter that Defendant sent Plaintiff Ashby about the Data Breach encouraged her to spend time mitigating the increased risk of harm.

143. Shortly after the Data Breach, in June of 2022, Plaintiff Ashby was alerted by the IRS that someone attempted to file a fraudulent tax return using her Private Information. As a result, Plaintiff Ashby's tax return was delayed, causing her to suffer injury from the lost time value of these funds. Furthermore, Plaintiff Ashby spent more than 8 hours dealing with this misuse, including speaking with the IRS.

144. Since the Data Breach, Plaintiff Ashby has received suspicious phone calls for medical services, including attempts to sell her a CPAP machine, which her health care providers have not prescribed or recommended. Prior to the data breach, she had not had any similar suspicious phone calls.

145. Plaintiff Ashby suffered actual injury in the form of damages to and diminution in the value of her Private Information—a form of intangible property that Plaintiff Ashby entrusted to Defendant, which was compromised in and as a result of the Data Breach.

146. As a result of the Data Breach, Plaintiff Ashby faces a substantial risk of

imminent harm that will remain the rest of her life. Plaintiff Ashby also faces a substantial risk of harm from a future Data Breach because her information remains, upon information and belief, inadequately protected in Defendant's possession. Plaintiff Ashby has a continuing interest in ensuring that her Private Information is protected from foreseeable future threats.

x. Plaintiff Margaret O'Grady

147. Plaintiff O'Grady is Defendant's current patient. Plaintiff O'Grady has provided Defendant with monetary compensation in exchange for medical services. Defendant also required Plaintiff O'Grady to provide it with her Private Information so that it could perform services and collect payment from her. Plaintiff O'Grady intended that a portion of the price she paid Defendant for services would be used to provide adequate data security. Defendant understood that Plaintiff O'Grady had this expectation, as evidenced by the statements in its NOPP and the sensitivity of the data it possessed.

148. Plaintiff O'Grady entrusted Defendant with her Private Information with the shared understanding that her information would be adequately protected from foreseeable threats. This shared understanding is evidenced from the Notice of Privacy Practices that she was provided and reviewed when receiving care. This shared understanding is further evidenced by the Privacy Policy on Defendant's website.

149. Upon information and belief, Plaintiff O'Grady's Private Information was stored on Defendant's network during the Data Breach and presently remains in Defendant's possession.

150. Defendant sent Plaintiff O'Grady a Notice Letter dated June 9, 2022, stating that its network was accessed by unauthorized third parties and indicating that Plaintiff O'Grady's Private Information was stolen during this event.

151. Plaintiff O'Grady is very careful about sharing her sensitive Private Information. Plaintiff O'Grady has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff O'Grady stores any documents containing her Private Information in a safe and secure location or destroys the documents.

152. Plaintiff O'Grady suffered an intangible privacy injury from the theft of her Private Information and its subsequent disclosure to third parties for criminal purposes. Plaintiff O'Grady's loss of privacy and the substantial risk of imminent harm Plaintiff O'Grady now faces has caused Plaintiff O'Grady to suffer proportionate fear and anxiety.

153. As a result of the Data Breach, Plaintiff O'Grady has spent hours dealing with the consequences of the Data Breach to mitigate and minimize her damages. This includes verifying the legitimacy of the notice of the Data Breach, exploring credit monitoring and identity theft protection services, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. Plaintiff O'Grady time spent on these matters is not only reasonable, but necessary; her failure to do so could result in her missing fraudulent activity and result in greater damages than she has already incurred. This time has been lost forever and cannot be recaptured. Even the Notice Letter that Defendant sent Plaintiff O'Grady about the Data Breach encouraged her to spend time mitigating the increased risk of harm.

154. Plaintiff O'Grady suffered actual injury in the form of damages to and diminution in the value of her Private Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

155. Since the Data Breach, Plaintiff O'Grady has also received an increase in

spam e-mails, text messages, and phone calls regarding medically related matters. Upon information and belief, this was because of the Data Breach, particularly given the timing and fact that much of the spam was medical related.

156. As a result of the Data Breach, Plaintiff O'Grady faces a substantial risk of imminent harm that will remain the rest of her life. Plaintiff O'Grady also faces a substantial risk of harm from a future Data Breach because her information remains, upon information and belief, inadequately protected in Defendant's possession. Plaintiff O'Grady has a continuing interest in ensuring that her Private Information is protected from foreseeable future threats.

xi. Plaintiff Mayra Esquivel and her minor son, E.N.

157. Plaintiff Esquivel and her minor son are Defendant's patients. Plaintiff Esquivel provided Defendant with monetary compensation in exchange for medical services. Defendant also required Plaintiffs to provide it with their Private Information so that Defendant could perform services and collect payment. Plaintiffs intended that a portion of the price they paid Defendant for services would be used to provide adequate data security. Defendant understood that Plaintiffs had this expectation, as evidenced by the statements in its NOPP and the sensitivity of the data it possessed.

158. Plaintiff Esquivel entrusted Defendant with her and E.N.'s Private Information with the shared understanding that her information would be adequately protected from foreseeable threats. This shared understanding is evidenced from the Notice of Privacy Practices that they were provided and reviewed when receiving care. This shared understanding is further evidenced by the Privacy Policy on Defendant's website.

159. Upon information and belief, Plaintiffs' Private Information was stored on Defendant's network during the Data Breach and presently remains in Defendant's

possession.

160. Defendant sent Plaintiff Esquivel and E.N. a Notice Letter dated June 9, 2022, stating that its network was accessed by unauthorized third parties and indicating that Plaintiffs' Private Information was stolen during this event.

161. Plaintiff Esquivel is very careful about sharing their sensitive Private Information. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff stores any documents containing their Private Information in a safe and secure location or destroys the documents.

162. Plaintiff Esquivel and E.N. suffered an intangible privacy injury from the theft of their Private Information and its subsequent disclosure to third parties for criminal purposes. Plaintiffs' loss of privacy and the substantial risk of imminent harm Plaintiff Esquivel and E.N. now face has caused Plaintiffs to suffer proportionate fear and anxiety.

163. Following the Data Breach, an unknown individual attempted to log into and use Plaintiff Esquivel's account for a Free Application for Federal Student Aid ("FAFSA").

164. Upon information and belief, Plaintiffs have spent a total of about ten (10) hours dealing with the consequences of the Data Breach, including but not limited to researching the events relating to and the effects of the Data Breach, investigating ways to mitigate damage done to them from Defendant's unauthorized disclosure of their Private Information, and precluding the attempted unauthorized use of Plaintiff Esquivel's FAFSA account. This time spent is not only reasonable, but necessary given that Plaintiffs had no other option but to spend time addressing and mitigating the fraud once they discovered it.

165. Plaintiff Esquivel and E.N. suffered actual injury in the form of damages to and diminution in the value of their Private Information—a form of intangible property

that Plaintiffs entrusted to Defendant, which was compromised in and as a result of the Data Breach.

166. Since the Data Breach, Plaintiff Esquivel has also received an increase in spam e-mails, text messages, and phone calls regarding medically related matters. Upon information and belief, this was because of the Data Breach, particularly given the timing and fact that much of the spam was medical related.

167. As a result of the Data Breach, Plaintiffs face a substantial risk of imminent harm that will remain the rest of their lives. Plaintiffs also face a substantial risk of harm from a future Data Breach because their information remains, upon information and belief, inadequately protected in Defendant's possession. Plaintiffs have a continuing interest in ensuring that their Private Information is protected from foreseeable future threats.

C. Plaintiffs and the Proposed Class Face Significant Risk of Continued Identity Theft

168. Plaintiffs and Class Members have suffered injury from the misuse of their Private Information that can be directly traced to Defendant. The ramifications of Defendant's failure to keep Plaintiffs' and the Class's Private Information secure are severe. According to experts, one out of four data breach notification recipients become a victim of identity fraud.[9]

169. As a result of Defendant's failures to prevent—and to timely detect—the Data Breach, Plaintiffs and the proposed Class have suffered and will continue to suffer

[9] *Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims*, THREATPOST.COM (Feb. 21, 2013), https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/ (last visited Dec. 1, 2024).

damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their Private Information is used;

b. The diminution in value of their Private Information;

c. The compromise and continuing publication of their Private Information;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Interference with the ability to access and use money or credit belonging to them;

f. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

g. Delay in receipt of tax refund monies;

h. Invasion of their privacy;

i. Unauthorized use of stolen Private Information; and

j. The continued risk to their Private Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the Privat Information in their possession.

170. PII has significant value in our increasingly digital economy. The value of consumer personal information is not derived solely (or even realistically) by its worth in some imagined marketplace where the consumer actually seeks to sell it to the highest

bidder, but rather in the economic benefit the consumer derives from being able to purchase goods and services remotely and without the need to pay in cash or a check. Indeed, the value of PII is key to unlocking many parts of the financial sector for consumers. Whether someone can obtain a mortgage, credit card, business loan, tax return, or even apply for a job depends on the integrity of their PII. However, because of YRMC's Data Breach the integrity and value of Plaintiffs' PII has significantly decreased.

171. The value of Plaintiffs' and the proposed Class's Private Information on the black market is considerable. Stolen Private Information trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

172. One such example of criminals using Private Information for profit is the development of "Fullz" packages.[10] Cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data

[10] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz", which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm*, KREBS ON SECURITY, (Sep. 18, 2014), https://krebsonsecurity.com/tag/fullz/ (last visited Dec. 1, 2024).

with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

173. This means that stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information was not included in the Private Information stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and other members of the proposed Class's stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

174. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Defendant did not rapidly report to Plaintiffs and the Class that their Private Information had been stolen.

175. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen Private Information. To protect themselves, Plaintiffs and the Class will need to be remain vigilant against unauthorized data use for years or even decades to come.

176. The Federal Trade Commission ("FTC") has issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has

noted the need to factor data security into all business decision-making.[11] According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.[12]

177. To that end, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. *See In the matter of Lookout Services, Inc.*, No. C-4326, ¶ 7 (June 15, 2011) ("[Defendant] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW, Inc.*, No. C-4157, ¶ 7 (Mar. 7, 2006) ("[Defendant] failed to employ sufficient measures to detect unauthorized access."); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008) ("[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's*

---

[11] *Start With Security, A Guide for Business*, FTC, https://www.ftc.gov/business-guidance/resources/start-security-guide-business (last visited Dec. 1, 2024).

[12] *Id.*

Inc., No. C-4291 (May 20, 2010) ("[Defendant] failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit access between instore networks . . ."). These orders, which all preceded the Data Breach, further clarify the measures businesses must take to meet their data security obligations. Defendant thus knew or should have known that its data security protocols were inadequate and were likely to result in the unauthorized access to and/or theft of Private Information.

178. The healthcare industry is a prime target for data breaches, which have continued to increase rapidly. According to the 2019 Healthcare Information and Management Systems Society Cybersecurity Survey, 68% of participating vendors reported having a significant security incident within the last 12 months, with a majority of those being caused by "bad actors."[13]

179. This can have a massive negative impact on victims. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[14]

180. The healthcare industry has "emerged as a primary target because [it sits] on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies to next of kin and credit cards, no

[13] *2019 HIMSS Cybersecurity Survey*, HEALTHCARE INFO. & MGMT. SYS. SOC'Y, INC. (Feb. 8, 2019), https://bit.ly/3LJqUr6 (last visited Dec. 1, 2024).

[14] Elinor Mills, *Study: Medical Identity Theft Is Costly for Victims*, CNET (Mar. 3, 2010), https://cnet.co/33uiV0v (last visited Dec. 1, 2024).

other organization, including credit bureaus, ha[s] so much monetizable information stored in their data centers."[15]

181. Medical-related identity theft is one of the most common, most expensive, and most difficult to prevent forms of identity theft. According to Kaiser Health News, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013[,]" which is more than identity thefts involving banking and finance, the government and the military, or education.[16]

182. "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place."[17] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market.[18]

183. When cybercriminals manage to steal health insurance information and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which Plaintiffs and Class Members are exposed.

---

[15] Eyal Benishti, *How to Safeguard Hospital Data from Email Spoofing Attacks*, INSIDE DIGITAL HEALTH (Apr. 4, 2019), https://bit.ly/3x6fz08 (last visited Dec. 1, 2024).

[16] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, KAISER HEALTH NEWS (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft/ (last visited Dec. 12, 2024).

[17] *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows*, IDX (May 14, 2015) https://www.idx.us/knowledge-center/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat (last visited Dec. 12, 2024).

[18] *Managing cyber risks in an interconnected world: Key findings from The Global State of Information Security Survey 2015*, PRICEWATERHOUSECOOPERS (Sept. 30, 2014), https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf (last visited Dec. 12, 2024); *see also* Brian Stack, *Here's How Much Your Personal Information is Selling for on the Dark Web*, EXPERIAN, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Dec. 12, 2024).

184. The Data Breach at issue here was targeted and financially motivated, as the only reason cybercriminals go through the trouble of hacking healthcare entities like Defendant is to steal the highly sensitive information they maintain, to exploit and sell for financial gain.

185. Charged with handling highly sensitive Personal Information including healthcare information, financial information, and insurance information, Defendant knew or should have known the importance of safeguarding the Personal Information that was entrusted to it. Defendant also knew or should have known of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Defendant's patients as a result of a breach. Defendant nevertheless failed to take adequate cybersecurity measures to prevent the Data Breach from occurring.

186. Defendant disclosed Plaintiffs' and Class Members' Private Information for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed Plaintiffs and Class Members' Private Information to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen Private Information.

187. Defendant's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for privacy, and has exposed the Private Information of Plaintiffs and potentially thousands of members of the proposed Class to unscrupulous operators, con artists, and outright criminals.

188. Defendant's failure to properly notify Plaintiffs and members of the proposed Class of the Data Breach exacerbated Plaintiffs' and members of the proposed Class's injury by depriving them of the earliest ability to take appropriate measures to protect their Private Information and take other necessary steps to mitigate the harm caused by the Data Breach.

D. Defendant Failed to Adhere to HIPAA

189. HIPAA prescribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[19]

190. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of Private Information are properly maintained.[20]

191. The Data Breach itself resulted from a combination of inadequacies showing Defendant failed to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

[19] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[20] *See* 45 C.F.R. § 164.306 (Security standards and General rules); 45 C.F.R. § 164.308 (Administrative safeguards); 45 C.F.R. § 164.310 (Physical safeguards); 45 C.F.R. § 164.312 (Technical safeguards).

a. Failing to ensure the confidentiality and integrity of electronic Private Information that it creates, receives, maintains, and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic Private Information in violation of 45 C.F.R. § 164.306(a)(2);

c. Failing to protect against any reasonably anticipated uses or disclosures of electronic Private Information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. Failing to ensure compliance with HIPAA security standards by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic Private Information to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to Private Information as necessary and appropriate for staff

members to carry out their functions and to maintain security of Private Information in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard Private Information, in compliance with 45 C.F.R. § 164.530(c).

E. Defendant Failed to Adhere to FTC Guidelines

192. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making.[21] To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of Personal Information.

193. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[22] The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

[21] *Start with Security: A Guide for Business*, FTC (June 2015), available at https://www.ftc.gov/business-guidance/resources/start-security-guide-business.

[22] *Protecting Personal Information: A Guide for Business*, FTC (Oct. 2016), available at https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.

194. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

195. The FTC recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[23]

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

197. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

CLASS ACTION ALLEGATIONS

198. Plaintiffs brings this action on behalf of themselves, and all members of the proposed Class (the "Class") pursuant to Federal Rule of Civil Procedure 23(b)(2) and (b)(3) as defined as:

> **All Yuma Regional Medical Center patients whose Private Information was accessed in the Data Breach.**

[23] *See Start with Security: A Guide for Business*, FTC (June 2015), available at https://www.ftc.gov/business-guidance/resources/start-security-guide-business.

199. The following people are excluded from the Class: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which Defendant or its parent has a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiffs' counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

200. The Class defined above is identifiable through Defendant's business records.

201. Plaintiffs reserve the right to amend the class definition.

202. This action is properly maintainable as a class action under Federal Rule of Civil Procedure 23.

203. **Numerosity.** Plaintiffs are representative of the proposed Class, consisting of hundreds of thousands of members, far too many to join in a single action.

204. **Commonality.** There are many questions of law and fact common to the claims of Plaintiffs and the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include, but are not necessarily limited to the following:

a. Whether Defendant had a duty to use reasonable care to safeguard Plaintiffs' and members of the Class's Private Information;

b. Whether Defendant breached the duty to use reasonable care to safeguard members of the Class's Private Information;

c. Whether Defendant breached its contractual promises to safeguard Plaintiffs' and members of the Class's Private Information;

d. Whether Defendant knew or should have known about the inadequacies of its data security policies and system and the dangers associated with storing sensitive Private Information;

e. Whether Defendant failed to use reasonable care and commercially reasonable methods to safeguard and protect Plaintiffs' and members of the Class's Private Information from unauthorized release and disclosure;

f. Whether the proper data security measures, policies, procedures, and protocols were in place and operational within Defendant's computer systems to safeguard and protect Plaintiffs' and members of the Class's Private Information from unauthorized release and disclosure;

g. Whether Defendant took reasonable measures to determine the extent of the Data Breach after it was discovered;

h. Whether Defendant's delay in informing Plaintiffs and members of the Class of the Data Breach was unreasonable;

i. Whether Defendant's method of informing Plaintiffs and other members of the Class of the Data Breach was unreasonable;

j. Whether Defendant's conduct was likely to deceive the public;

k. Whether Defendant is liable for negligence or gross negligence;

l. Whether Defendant's conduct, practices, statements, and representations about the Data Breach of the Private Information violated applicable state laws;

m. Whether Plaintiffs and members of the Class were injured as a proximate cause or result of the Data Breach;

n. Whether Plaintiffs and members of the Class were damaged as a proximate cause or result of Defendant's breach of its contract with Plaintiffs and members of the Class;

o. Whether Defendant's practices and representations related to the Data Breach breached implied warranties;

p. What the proper measure of damages is; and

q. Whether Plaintiffs and members of the Class are entitled to restitutionary, injunctive, declaratory, or other relief.

205. **Typicality.** Plaintiffs' claims are typical of the claims of other members of the Class in that Plaintiffs, and the members of the Class sustained damages arising out of Defendant's Data Breach, wrongful conduct and misrepresentations, false statements, concealment, and unlawful practices, and Plaintiffs and members of the Class sustained similar injuries and damages, as a result of Defendant's uniform illegal conduct.

206. **Adequacy of Representation.** Plaintiffs will fairly and adequately represent and protect the interests of the Class and has retained counsel competent and experienced in complex class actions to vigorously prosecute this action on behalf of the Class. Plaintiffs have no interests that conflict with, or are antagonistic to those of, the Class, and Defendant has no defenses unique to Plaintiffs.

207. **Superiority of Class Action.** A class action is also a fair and efficient method of adjudicating the controversy because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy as joinder of all parties is impracticable. The damages suffered by the individual members of the Class

will likely be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's actions. Thus, it would be virtually impossible for the individual members of the Class to obtain effective relief from Defendant's misconduct. Even if members of the Class could sustain such individual litigation, it would still not be preferable to a class action, because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Consolidated Class Action Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Economies of time, effort, and expense will be fostered, and uniformity of decisions ensured.

208. A class action is therefore superior to individual litigation because:

a. The amount of damages available to an individual Plaintiff is insufficient to make litigation addressing Defendant's conduct economically feasible in the absence of the class action procedural device;

b. Individualized litigation would present a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system; and

c. The class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

209. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable

identities of Class members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

210. Adequate notice can be given to Class members directly using information maintained in Defendant's records.

211. **Predominance**. Pursuant to Rule 23(b)(3), the issues in this action are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include but are not limited to the questions identified above.

212. This proposed class action does not present any unique management difficulties.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiffs and the Class)

213. Plaintiffs re-allege and incorporate by reference the allegations contained in paragraphs 1-212 as if fully alleged at length herein.

214. Defendant knowingly and intentionally acquired, possessed, and maintained Plaintiffs' and Class Members' Private Information and had a duty to safeguard and protect that information from unauthorized access and/or disclosure.

215. Defendant voluntarily assumed responsibility over Plaintiffs' and Class Members' Private Information and did so for commercial purposes in conducting its ordinary course of business as a medical provider.

216. Plaintiffs and Class Members entrusted Defendant with their Private Information as a condition of receiving medical care from Defendant, and under the impression that Defendant would exercise reasonable care in maintaining their Private

Information.

217. Defendant had a duty under common law to adopt and employ procedures to detect and prevent the loss of unauthorized access of Plaintiffs' and Class Members' sensitive and confidential Private Information.

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

219. Moreover, under HIPAA (42 U.S.C. § 1302d, *et seq*.), Defendant had a duty to implement reasonable safeguards to protect Plaintiffs' and Class members' Private Information. Specifically, Defendant had a duty to render the electronic Private Information it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 C.F.R. § 164.304 definition of encryption).

220. The Hippocratic Oath acknowledges the physician's obligation to keep in trust patient confidences. Further, Principle IV of the American Medical Association's Principles of Medical Ethics requires physicians to "safeguard patient confidences within the constraints of the law." Finally, Section 5.05 of the Current Opinions of the Judicial Council of the American Medical Association states that "[t]he information disclosed to a physician during the course of the relationship between physician and patient is confidential to the greatest possible degree."

221. Furthermore, "all medical records and payment records, and the information contained in medical records and payment records, are privileged and confidential" under Arizona law. Ariz. Stat. § 12-2292(A).

222. Defendant's own policies, which state Defendant is committed to protecting patient data, also evidence a duty.

223. Defendant had a duty to exercise reasonable care in handling and using the Private Information that it collected and maintained in providing medical care, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

224. At all relevant times, Defendant was fully aware of the sensitive nature of Plaintiffs' and Class Members' Private Information that it maintained, as well as the types of harm that Plaintiffs and Class Members would suffer were their Private Information to be wrongfully accessed, disclosed and/or exfiltrated.

225. At all relevant times, it was foreseeable that Defendant's failure to adequately safeguard Plaintiffs' and Class Members' Private Information in accordance with state-of-the-art industry standards concerning data security would result in the compromise of their Private Information. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and Class Members' Private Information by disclosing and providing access to this information to third parties and by failing to properly supervise both the manner in which the Private Information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

226. Defendant owed Plaintiffs and Class Members a duty to notify them within a reasonable time frame of any breach to the security of their Private Information. This

includes a duty to timely and accurately disclose the scope, nature, and occurrence of the Data Breach. This duty is required and necessary in order for Plaintiffs and members of the Class to take appropriate measures to protect their Private Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps in an effort to mitigate the harm caused by the Data Breach.

227. Defendant owed these duties to Plaintiffs and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiffs' and members of the Class's personal information and Private Information for medical treatment services. Plaintiffs and members of the Class were required to provide their personal information and Private Information to Defendant in order to receive medical treatment and services, and Defendant retained that information.

228. By assuming possession of Plaintiffs' and Class Members' Private Information for monetary gain and in its ordinary course of business, Defendant had a duty of care to secure and safeguard their network, as well as the Private Information stored within it, to prevent unauthorized disclosure. This duty includes Defendant's responsibility to employ measures that assist with breach detection and provide timely notice to affected parties.

229. The risk that unauthorized persons would attempt to gain access to the Private Information and misuse it was foreseeable. Given that Defendant holds vast amounts of Private Information, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the Private Information.

230. Private Information is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Private Information of Plaintiffs and members of the Class and the importance of exercising reasonable care in handling it.

231. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and Private Information of Plaintiffs and members of the Class which actually and proximately caused the Data Breach and Plaintiffs' and members of the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs' and members of the Class's injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and members of the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

232. Defendant's negligence actually and proximately caused Plaintiffs' and Class Members' actual, tangible, injuries-in-fact and damages, including, without limitation, the theft of their Private Information by criminals, improper disclosure of their Private Information, their lost access to their monetary and/or monetary accounts arising from fraud; lost benefit of their bargain, lost value of their Private Information, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, their loss of access and use of their money and/or monetary accounts resulting from fraudulent activity caused by the Data Breach;

the injuries-in-fact and damages which are still ongoing, imminent, immediate, and which they continue to face.

SECOND CAUSE OF ACTION
Breach of Implied Contract/Implied Duty of Good Faith and Fair Dealing
(On Behalf of Plaintiffs and the Class)

233. Plaintiffs re-allege and incorporate by reference the allegations contained in paragraphs 1-212 as if fully alleged at length herein.

234. Plaintiffs and Class Members are Defendant's current and former patients. As Defendant's patients, Plaintiffs and Class Members agreed to provide Defendant with monetary compensation in exchange for medical services. During the course of this relationship, Defendant required Plaintiffs and Class Members to provide it with their Private Information so that it could perform services and collect payment on medical debts.

235. Implied within the agreement for Defendant to provide medical services in exchange for monetary compensation and Private Information was a covenant to adequately protect Plaintiff's Private Information from foreseeable threats.

236. Plaintiffs and Class Members intended for a portion of the money that they paid Defendant for services to be used for implementing and maintaining adequate data security practices. When Defendant failed to use this money for adequate data security, Plaintiffs and Class Members lost the benefit of their bargain with Defendant.

237. In the privacy policy on its website and the notice of privacy practices that it provides patients during treatment, Defendant expressly promised that it would not disclose the Private Information it collects from patients to unauthorized persons. Defendant also promised to maintain safeguards to protect its patients' Private Information.

238. Implicit in the agreement between Plaintiffs and Class Members and Defendant was Defendant's obligation to (a) use their Private Information for necessary

purposes only; (b) take reasonable steps to safeguard their Private Information; (c) prevent unauthorized access and disclosure of their Private Information; (d) provide Plaintiffs and Class Members with prompt and adequate notice of any and all unauthorized access to and/or theft of their Private Information; (e) employ reasonable safeguards to protect the Private Information from unauthorized disclosure and/or misuse; and (f) retain the Private Information only under conditions that kept the information secure and confidential.

239. Plaintiffs and Class Members manifested mutual assent by providing their money and Private Information. Defendant manifested mutual assent by performing medical services, collecting Plaintiffs' and Class Members' Private Information, and then using it to collect payment and perform services.

240. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of such agreement to keep their information reasonably secure or in the absence of an implied promise to monitor its computer systems and networks to ensure that the medical information maintained and belonging to its patients was reasonably secure.

241. Defendant materially breached the contract(s) it had with Plaintiffs and members of the Class (and the duty of good faith and fair dealing contained therein) by failing to adequately safeguard such information and failing to notify Plaintiffs and Class Members promptly of the intrusion into Defendant's systems that compromised such information.

242. The damages sustained by Plaintiffs and Class Members as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

243. Plaintiffs and Class Members have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendant.

244. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter —of the bargain.

245. Plaintiffs and Class Members fully performed their obligations under the implied contract with Defendant. Defendant did not. Plaintiffs and Class Members would not have provided their confidential Private Information to Defendant in the absence of their implied contracts with Defendant and would have instead retained the opportunity to control their Private Information for uses other than medical treatment, billing, and benefits from Defendant.

246. Defendant failed to advise Plaintiffs and Class Members of the Data Breach within a reasonable amount of time.

247. Defendant's conduct violated the duty of good faith and fair dealing in its agreements with Plaintiffs and Class Members.

248. Plaintiffs and Class Members have sustained damages as a result of Defendant's breaches of its agreement, including breaches thereof through violations of the covenant of good faith and fair dealing.

THIRD CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

249. Plaintiffs re-allege and incorporate by reference the allegations contained in

paragraphs 1-212 as if fully alleged at length herein.

250. This claim is pleaded in the alternative to the breach of implied contract claim.

251. Defendant benefitted from the receipt of Plaintiffs' and Class Members' Private Information by its ability to possess and use that information for its own benefit, including its business purposes (like payment collection).

252. Defendant also received a benefit from the compensation that Plaintiffs and Class Members paid for medical services (or the money that was paid on their behalf), which should have (in part) been used to fund adequate data security practices.

253. Defendant knew and understood these benefits. In acknowledging these benefits, Defendant also understood and appreciated that Plaintiffs' and Class Members' Private Information was private and confidential, and that its value depended upon Defendant's maintaining the privacy and confidentiality of that information.

254. Defendant failed to provide or implement reasonable security safeguards or protections for Plaintiffs' and Class Members' Private Information.

255. Under principals of equity and good conscience, Defendant should not be permitted to retain the money and the value of the Private Information belonging to Plaintiffs and Class Members because Defendant failed to implement and follow adequate data security measures, as discussed throughout this Complaint.

256. Defendant wrongfully accepted and retained benefits at Plaintiffs' and Class Members' detriment. This enrichment is at Plaintiffs' and Class Members' expense, and is unjust.

257. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and members of the Class all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged herein.

FOURTH CAUSE OF ACTION
Breach of Fiduciary Duty

258. Plaintiffs re-allege and incorporate by reference the allegations contained in paragraphs 1-212 as if fully alleged at length herein.

259. There is a fiduciary relationship between the physician and patient that requires the physician to exercise the utmost good faith. The physician's fiduciary duty requires they act in the best interests of the patient so as to protect the sanctity of the physician-patient relationship.

260. The Hippocratic Oath acknowledges the physician's obligation to keep in trust patient confidences. Further, Principle IV of the American Medical Association's Principles of Medical Ethics requires physicians to "safeguard patient confidences within the constraints of the law." Finally, Section 5.05 of the Current Opinions of the Judicial Council of the American Medical Association states that "[t]he information disclosed to a physician during the course of the relationship between physician and patient is confidential to the greatest possible degree."

261. Moreover, under HIPAA (42 U.S.C. § 1302d, *et seq*.), Defendant had a duty to implement reasonable safeguards to protect Plaintiffs' and Class members' Private Information. Specifically, Defendant had a duty to render the electronic Private Information it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning

without use of a confidential process or key" (45 C.F.R. § 164.304 definition of encryption).

262. Furthermore, "all medical records and payment records, and the information contained in medical records and payment records, are privileged and confidential" under Arizona law. Ariz. Stat. § 12-2292(A).

263. Defendant violated its fiduciary duty to Plaintiffs and Class Members by not implementing and maintaining adequate data security measures, as discussed throughout this Complaint.

264. Defendant's breaches of its fiduciary duty have proximately caused Plaintiffs and Class Members to suffer injuries as described in this Complaint.

FIFTH CAUSE OF ACTION
Arizona Consumer Fraud Act,
A.R.S. §§ 44-1521, *et seq.*
(On Behalf of Plaintiffs and the Class)

265. Plaintiffs re-allege and incorporate by reference the allegations contained in paragraphs 1-212 as if fully alleged at length herein.

266. Defendant sold Plaintiffs and Class members "merchandise" as that term is defined by A.R.S. § 44-1521, in the form of services, including healthcare and insurance services, as well as the sale of objects, wares, goods, and commodities at outlets where Defendant accepted payment cards in point-of-sale transactions.

267. Section 44-1522 of the Arizona Consumer Fraud Act provides:

> The act, use or employment by any person of any deception, deceptive or unfair act or practice, fraud, false pretense, false promise, misrepresentation, or concealment, suppression or omission of any material fact with intent that others rely on such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise whether or not any person has in fact been misled, deceived or damaged thereby.

See A.R.S. § 44-1522(A).

268. Defendant used deception, used a deceptive act or practice, and fraudulently omitted and concealed material facts in connection with the sale or advertisement of that merchandise in violation of A.R.S. § 44-1522(A).

269. Defendant omitted and concealed material facts, which it knew about and had the duty to disclose—namely, Defendant's inadequate privacy and security protections and safeguards for Plaintiffs' and Class Members' Private Information, including insufficient cybersecurity safeguards, staff, and training.

270. Defendant omitted and concealed those material facts in its NOPP even though in equity and good conscience those facts should have been disclosed and did so with the intent that others would rely on the omission, suppression, and concealment. This is underscored by the fact that Defendant is a hospital and thus has an inherent duty of confidentiality, leading Plaintiffs and Class Members to trust Defendant's representations as true.

271. Separately, Defendant engaged in unfair acts and practices in violation of the ACFA by failing to implement and maintain reasonable security measures and secure Plaintiffs' Private Information in a manner compliant and consistent with applicable laws, regulations, and industry standings. This violates established public policy, is immoral, unethical, and injurious to Defendant's consumers and patients.

272. The concealed facts are material in that they are logically related to the transactions at issue and rationally significant to the parties in view of the nature and circumstances of those transactions.

273. Defendant knew or should have known that its computer system and data security practices were inadequate to safeguard Plaintiffs' and Class members' Private

Information, and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in these deceptive acts and practices were negligent, knowing and willful, and wanton and reckless with respect to the rights of Plaintiffs and Class members.

274. Specifically, Defendant failed to comply with the standards outlined by the FTC and HIPAA regarding protecting Private Information. As a healthcare institution that has operated since 1964, Defendant was or should have been aware of these standards. Defendant's data security systems did not comply with the FTC's guidelines and HIPAA's Administrative Simplification Rules and, as a result, were operating below the minimum standards set forth.

275. Plaintiffs and Class members were ignorant of the truth and relied on the concealed facts and incurred damages as a consequent and proximate result.

276. Plaintiffs and Class members seek all available relief under A.R.S. §§ 4421, *et seq.*, including, but not limited to, compensatory damages, punitive damages, injunctive relief, and attorneys' fees and costs.

PRAYER FOR RELIEF

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

A. An Order certifying this action as a class action and appointing Plaintiffs as Class representatives and the undersigned as Class counsel;

B. A mandatory injunction directing Defendant to adequately safeguard the Private Information of Plaintiffs and the Class hereinafter by implementing improved security procedures and measures;

C. A mandatory injunction requiring that Defendant provide notice to each member of the Class relating to the full nature and extent of the Data Breach and the disclosure of Private Information to unauthorized persons;

D. Enjoining Yuma Regional from further deceptive practices and making untrue statements about the Data Breach and the stolen Private Information;

E. An award of damages, in an amount to be determined;

F. An award of attorneys' fees and costs;

G. An award of pre- and post-judgment interest, costs, attorneys' fees, expenses, and interest as permitted by law;

H. Granting the Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and,

I. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all issues so triable.

Dated: December 13, 2024

Respectfully submitted,

/s/ Bryan L. Bleichner

CHESTNUT CAMBRONNE PA
Bryan L. Bleichner (admitted *pro hac vice*)
Philip J. Krzeski (admitted *pro hac vice*)
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Telephone: (612) 339-7300
Fax: (612) 336-2940
bbleichner@chestnutcambronne.com
pkrzeski@chestnutcambronne.com

Jean S. Martin (admitted *pro hac vice*)
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Fax: (813) 223-5402
jeanmartin@forthepeople.com

Interim Co-Lead Class Counsel for Plaintiffs and the Proposed Class

CERTIFICATE OF SERVICE

I hereby certify that on December 13, 2024, a copy of foregoing was filed electronically. Notice of this filing will be sent by operation of the Court's electronic filing system to all parties indicated on the electronic filing receipt. Parties may access this filing through the Court's system.

/s/ Bryan L. Bleichner
Bryan L. Bleichner