Cristina Perez Hesano (#027023)
PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301
Telephone: (602) 730-7100
Fax: (602) 794-6956
cperez@perezlawgroup.com

Nicholas A. Migliaccio (pro hac vice forthcoming)
Jason Rathod (pro hac vice forthcoming)
Tyler Bean (pro hac vice forthcoming)
Kevin Leddy (pro hac vice forthcoming)
MIGLIACCIO & RATHOD, LLP
412 H Street NE
Washington, D.C. 20002
202.470.3520
nmigliaccio@classlawdc.com
Attorneys for Plaintiffs

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ARIZONA

Carol Ashby and Keith Gren, on behalf of themselves and all others similarly situated, **Plaintiffs,** **vs.** **Yuma Regional Medical Center,** **Defendant.**	**Case No.** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Carol Ashby ("Plaintiff Ashby" or "Ms. Ashby") and Keith Gren ("Plaintiff Gren" or "Mr. Gren") (collectively, "Plaintiffs"), individually and on behalf of all others similarly situated, through the undersigned counsel, hereby allege the following against Defendant Yuma Regional Medical Center ("YRMC" or "Defendant").

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

NATURE OF THE ACTION

1. This is a class action for damages with respect to Yuma Regional Medical Center, for its failure to exercise reasonable care in securing and safeguarding its patients' sensitive personal data—including Social Security numbers, health insurance identifications numbers, demographic information, and other medical information related to patient care (collectively, the "Private Information").

2. This class action is brought on behalf of patients whose sensitive Private Information was stolen by cybercriminals in a cyber-attack that accessed sensitive patient information through YRMC's networks and systems between April 21, 2022 and April 25, 2022 (the "Data Breach").

3. YRMC reported to Plaintiffs that information compromised in the Data Breach included their Private Information.

4. Plaintiffs were not notified until June of 2022, nearly two months after their information was first accessed.

5. As a result of the Data Breach, Plaintiffs and other "Class" (defined below) members have experienced and will continue to experience various types of misuse of their Private Information in the coming years, including but not limited to unauthorized credit card charges, unauthorized access to email accounts, and other fraudulent use of their financial information.

6. There has been no assurance offered from YRMC that all personal data or copies of data have been recovered or destroyed. YRMC offered Experian IdentityWorks Credit 3B credit monitoring for one year, which falls far short of guaranteeing the security of Plaintiffs' information. To mitigate further harm, Plaintiffs chose not to disclose any more information to receive services connected with YRMC.

7. Accordingly, Plaintiffs assert claims for negligence, breach of contract, breach of implied contract, unjust enrichment, breach of fiduciary duty, and violations of Arizona consumer protection statutes.

PARTIES

A. Plaintiff Carol Ashby

8. Plaintiff Carol Ashby is a citizen and resident of Yuma, Arizona. Ms. Ashby was a patient of YRMC for diagnostic testing services and x-ray services at YRMC, including for a number of tests that she had performed in and around September of 2021. Ms. Ashby's Private Information was therefore stored on YRMC's systems at all times material hereto. Plaintiff Ashby received notice letters from YRMC notifying her that her Private Information was stolen in the Data Breach.

9. The June 9, 2022 Notice Letter Plaintiff Ashby received from YRMC notified her that cybercriminals obtained her Private Information.

10. The affects of the data breach occurred before Ms. Ashby was aware that her information was affected. After scheduling a doctor's appointment on the week of April 18, 2022, Ms. Ashby arrived at a Yuma Regional facility to find out that her appointment had been cancelled, that she no longer had use of the hospital's patient portal, and that the medical staff had no record of her appointment. Hospital staff mentioned that the institution's systems were affected and that they likely would not be able to reschedule her appointment until a later date. It took several weeks for Ms. Ashby's appointment to be rescheduled.

11. Since the Data Breach, Plaintiff Ashby received a notification from the Internal Revenue Service dated June 2, 2022, informing her that an unauthorized individual filed a tax return in her name for the 2021 tax year without her permission. Ms. Ashby neither authorized nor approved of any individual filing a tax return in her name, and while the IRS has placed a fraud alert in its system related to Ms. Ashby's Tax Identification Number, Ms. Ashby has not been able to determine who could have filed the return in her name or whether a check has been

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

sent to an unauthorized party. It is therefore indisputable that Ms. Ashby has experienced damages related to the breach and is at a substantial risk of future harm.

12. Since the data breach, Ms. Ashby has spent approximately five hours on the phone with credit agencies and the IRS, attempting to determine whether her other accounts have been compromised.

13. Although some of these harms have already occurred in Ms. Ashby's case, the worst may be yet to come. In the months and years following the Data Breach, Ms. Ashby and the other Class members will experience a slew of harms as a result of Defendant's ineffective data security measures. Some of these harms will include fraudulent charges, medical procedures ordered in patients' names without their permission, and targeted advertising without patient consent.

14. Plaintiff Ashby greatly values her privacy, especially in receiving medical services, and would not have visited YRMC facilities if she had known that her Private Information would be maintained using inadequate data security systems.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

B. Plaintiff Keith Gren

15. Plaintiff Keith Gren is a citizen and resident of Yuma, Arizona. Plaintiff Gren has been a patient at YRMC, including for an emergency room visit in February of 2022, and his Private Information was stored on YRMC's systems at all times material hereto. Plaintiff Gren received a Notice Letter from YRMC notifying him that his Private Information was stolen in the Data Breach.

16. The Notice Letter Plaintiff Gren received from YRMC notified him that cybercriminals obtained his Private Information.

17. In the months and years following the Data Breach, Mr. Gren and the other Class members will experience a slew of harms similar to those already experienced by Plaintiff Ashby as a result of Defendant's ineffective data security measures. Some of these harms will include

fraudulent charges, medical procedures ordered in patients' names without their permission, and targeted advertising without patient consent.

18. Plaintiff Gren greatly values his privacy, especially in receiving medical services, and would not have visited YRMC facilities if he had known that his Private Information would be maintained using inadequate data security systems

C. Defendant

19. Defendant Yuma Regional Medical Center is a comprehensive healthcare company that offers medical services to the residents of Yuma, Arizona, and the surrounding areas. YRMC operates dozens of facilities throughout Yuma and provides healthcare services to thousands of patients a year. YRMC's Headquarters is located at 101 East Second Street, Yuma, Arizona 85364. YRMC's policies and practices, including those used for data privacy, are established in, and emanate from, Arizona.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

JURISDICTION AND VENUE

20. The 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 of 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.

21. The Court has personal jurisdiction over Defendant because Defendant is headquartered in Arizona and conducts substantial business in this District.

22. Venue is proper in this Court pursuant to 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.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

FACTS

23. Defendant provides healthcare services to thousands of patients per year. As part of its services, YRMC was entrusted with, and obligated to safeguard and protect the Private Information of Plaintiffs and the Class in accordance with all applicable laws.

24. In April of 2022, Defendant first learned of an unauthorized entry into its network, which contained patients' Private Information including names, Social Security numbers, and medical information. YRMC posted the following notice on its website:[1]

> Yuma Regional Medical Center (YRMC) is committed to protecting the privacy and security of our patients' information. Regrettably, we recently addressed a cybersecurity incident that involved some of that information. This notice explains the incident and the measures we have taken in response:
>
> **What Happened:** On April 25, 2022, we identified a ransomware incident affecting some internal systems. Upon detecting the incident, YRMC took immediate action, taking systems offline, communicating with law enforcement, and initiating an investigation with the help of a third-party forensic firm. The investigation determined that an unauthorized person gained access to our network between April 21, 2022, and April 25, 2022, and removed a subset of files from our systems.
>
> **What Information was Involved:** The files contained certain patient information, including names, Social Security numbers, health insurance information and limited medical information relating to care as a YRMC patient. Our electronic medical record application was not accessed during this incident.
>
> **What We are Doing in Response:** We want to assure our community that we are taking this matter very seriously. To 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.

[1] Yuma Regional Medical Center, *Notice of Data Breach*, https://www.yumaregional.org/EmergeWebsite/media/Yuma-Documents/Yuma-Regional-Medical-Center-Notice.pdf/ (last visited July 18, 2022).

> We are mailing letters to affected patients and offering free credit monitoring and identify theft protection services to those who are eligible. If you believe you are affected and do not receive a letter by July 10, 2022, please contact our dedicated external call center at (855) 503-3409, Monday through Friday, 6:00 a.m. to 3:30 p.m., Pacific Time.

25. Upon learning of the Data Breach in April of 2022, Defendant investigated. As a result of the Data Breach, Defendant initially estimated that the Private Information of at least 737,448 patients, each of which had previously received services from Defendant, was potentially compromised.[1]

26. In June of 2022, Defendant first announced that it learned of suspicious activity that allowed one or more cybercriminals to access its systems through a ransomware attack. The 2022 Notice disclosed that suspicious activity on the company's network enabled a threat actor to access YRMC systems.

27. Defendant offered no explanation for the delay between the initial discovery of the Breach and the belated notification to affected patients, which resulted in Plaintiffs and Class members suffering harm they otherwise could have avoided had a timely disclosure been made.

28. YRMC's notice of Data Breach was not just untimely but woefully deficient, failing to provide basic details of the Breach, including but not limited to, how unauthorized parties accessed its networks, whether the information was encrypted or otherwise protected, how Defendant learned of the Data Breach, whether the Breach occurred system-wide, whether servers storing information were accessed, and how many patients were affected by the Data Breach. Even worse, YRMC offered only one year of identity monitoring Plaintiffs and Class

[1] These numbers were reported to the Health and Human Services Healthcare Data Breach Portal. *See Cases Currently Under Investigation*, U.S. DEP'T OF HEALTH & HUMAN SERVS.: BREACH PORTAL, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf [hereinafter *Breach Portal*] (last visited July 18, 2022).

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

members, which required the disclosure of additional Private Information to a YRMC-associated third-party, with which Private Information YRMC had just demonstrated it could not be trusted.

29. Plaintiffs' and Class members' Private Information is for sale to criminals on the dark web, meaning that unauthorized parties have already accessed and viewed Plaintiffs' and Class members' unencrypted, unredacted information, including names, Social Security numbers, health information, and more.

30. The Breach occurred because Defendant failed to take reasonable measures to protect the Private Information it collected and stored. Among other things, Defendant failed to implement data security measures designed to prevent this attack, despite repeated warnings to the healthcare industry, insurance companies, and associated entities about the risk of cyberattacks and the highly publicized occurrence of many similar attacks in the recent past on other healthcare providers.

31. Defendant disregarded the rights of Plaintiffs and Class members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiffs' and Class members' Private Information was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the Private Information of Plaintiffs and Class members was compromised through unauthorized access by an unknown third party. Plaintiffs and Class members have a continuing interest in ensuring that their information is and remains safe.

A. Defendant's Privacy Promises

32. YRMC made various promises to its patients, including Plaintiffs and Class members, that it would maintain the security and privacy of their Private Information.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

33. In its Notice of Privacy Practices, Defendant stated under a section bolded and titled "How Will We Use and Disclose Your Medical Information?" some of the following:[1]

- Treatment
- Appointments
- Patient Directory
- Family Members and Others Involved in Your Care
- Payment
- Hospital Operations
- Public Safety

34. YRMC describes how it may use and disclose medical information for each category of uses or disclosures, none of which provide it a right to expose patients' Private Information in the manner it was exposed to unauthorized third-party cybercriminals in the Data Breach.

35. By failing to protect Plaintiffs' and Class members' Private Information, and by allowing the Data Breach to occur, YRMC broke these promises to Plaintiffs and Class members.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

B. Defendant Failed to Maintain Reasonable and Adequate Security Measures to Safeguard Patients' Private Information

36. YRMC acquires, collects, and stores a massive amount of its patients' protected Private Information, including health information and other personally identifiable data.

37. As a condition of engaging in health-related services, YRMC requires that these patients entrust it with highly confidential Private Information.

38. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class members' Private Information, YRMC assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class members' Private Information from disclosure.

[1] Yuma Regional Medical Center, *Notice of Privacy* Practices, https://www.yumaregional.org/EmergeWebsite/media/Yuma-Documents/NoticePrivacyPracticesEnglish.pdf (last visited July 18, 2022).

39. Defendant had obligations created by the Health Insurance Portability Act (42 U.S.C. § 1320d *et seq.*) ("HIPAA"), industry standards, common law, and representations made to Class members, to keep Class members' Private Information confidential and to protect it from unauthorized access and disclosure.

40. Defendant failed to properly safeguard Class members' Private Information, allowing hackers to access, view, and exfiltrate their Private Information.

41. Plaintiffs and Class members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant and any of its affiliates would comply with their obligation to keep such Information confidential and secure from unauthorized access.

42. Prior to and during the Data Breach, Defendant promised patients that their Private Information would be kept confidential.

43. Defendant's failure to provide adequate security measures to safeguard patients' Private Information is especially egregious because Defendant operates in a field which has recently been a frequent target of scammers attempting to fraudulently gain access to patients' highly confidential Private Information.

44. In fact, Defendant has been on notice for years that the healthcare industry and health insurance companies are a prime target for scammers because of the amount of confidential patient information maintained.

45. Defendant was also on notice that the FBI has been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[1]

46. The American Medical Association ("AMA") has also warned healthcare companies about the important of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[2]

47. The number of US data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year.[3] In 2017, a new record high of 1,579 breaches were reported—representing a 44.7 percent increase.[4] That trend continues.

48. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[5] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. 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

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

---

[1] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warnshealthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820.

[2] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED. ASS'N (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals.

[3] Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), https://www.idtheftcenter.org/surveys-studys.

[4] Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review*, https://www.idtheftcenter.org/2017-data-breaches/.

[5] Identity Theft Resource Center, *2018 End -of-Year Data Breach Report*, https://www.idtheftcenter.org/2018-data-breaches/.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

out-of-pocket costs for healthcare they did not receive in order to restore coverage.[1] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the victims were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[2]

49. A 2017 study conducted by HIMSS Analytics showed that email was the most likely cause of a data breach, with 78 percent of providers stating that they experienced a healthcare ransomware or malware attack in the past 12 months.

50. Healthcare related data breaches continued to increase rapidly into 2021 when YRMC's systems were breached.[3]

51. In the Healthcare industry, the number one threat vector from a cyber security standpoint is phishing. Cybersecurity firm Proofpoint reports that "phishing is the initial point of compromise in most significant [healthcare] security incidents, according to a recent report from the Healthcare Information and Management Systems Society (HIMSS). And yet, 18% of healthcare organizations fail to conduct phishing tests, a finding HIMSS describes as "incredible."[4]

52. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precaution for protection."[5]

---

[1] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for- victims/.
[2] *Id.*
[3] *2019 HIMSS Cybersecurity Survey*, https://www.himss.org/2019-himsscybersecurity-survey.
[4] Aaron Jensen, *Healthcare Phishing Statistics: 2019 HIMSS Survey Results*, PROOFPOINT (Mar. 27, 2019), https://www.proofpoint.com/us/security-awareness/post/healthcare-phishingstatistics-2019-himss-survey-results.
[5] *See How to Protect Your Networks from RANSOMWARE*, FBI (2016) https ://www. fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

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

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege; no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

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

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks . . .

- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net) . . .

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it . . .

- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic . . .[1]

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

- **Secure internet-facing assets**
  - Apply the latest security updates
  - Use threat and vulnerability management
  - Perform regular audit; remove privilege credentials;

- **Thoroughly investigate and remediate alerts**

[1] *See Security Tip (ST19-001) Protecting Against Ransomware*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (Apr. 11, 2019), https://us-cert.cisa.gov/ncas/tips/ST19-001.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

- Prioritize and treat commodity malware infections as potential full compromise

- **Include IT Pros in security discussions**
  - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

- **Build credential hygiene**
  - use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

- **Apply principle of least-privilege**
  - Monitor for adversarial activities
  - Hunt for brute force attempts
  - Monitor for cleanup of Event Logs
  - Analyze logon events

- **Harden infrastructure**
  - Use Windows Defender Firewall
  - Enable tamper protection
  - Enable cloud-delivered protection
  - Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[1]

56. These are basic, common-sense email security measures that every business, not only healthcare businesses, should be doing. YRMC, with its heightened standard of care should be doing even more. But by adequately taking these common-sense solutions, YRMC could have prevented this Data Breach from occurring.

[1] *See Human-operated ransomware attacks: A preventable disaster*, MICROSOFT (Mar. 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-apreventable-disaster/.

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

58. With respect to training, YRMC specifically failed to:

- Implement a variety of anti-ransomware training tools, in combination, such as computer-based training, classroom training, monthly newsletters, posters, login alerts, email alerts, and team-based discussions;
- Perform regular training at defined intervals such as bi-annual training and/or monthly security updates; and
- Craft and tailor different approaches to different employees based on its base knowledge about technology and cybersecurity.

59. The Private Information was also maintained on YRMC's computer system in a condition vulnerable to cyberattacks such as through the infiltration of Defendant's systems through ransomware attacks. The mechanism of the cyberattack and the potential for improper disclosure of Plaintiffs' and Class members' Private Information was a known risk to YRMC, and thus YRMC was on notice that failing to take reasonable steps necessary to secure the Private Information from those risks left the Private Information in a vulnerable position.

C. The Monetary Value of Privacy Protections and Private Information

60. The fact that Plaintiffs' and Class members' Private Information was stolen—and was offered for sale to cyber criminals—demonstrates the monetary value of the Private Information.

61. At all relevant times, Defendant was well aware that Private Information it collects from Plaintiffs and Class members is highly sensitive and of significant value to those who would use it for wrongful purposes.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

62. Private Information is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and medical and financial fraud.[1] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII and PHI on multiple underground Internet websites, commonly referred to as the dark web.

63. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[2]

64. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 Billion per year online advertising industry in the United States.[3]

65. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

[1] Federal Trade Commission, *Warning Signs of Identity Theft* (Sept. 2018), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft .

2 *Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data*, FED. TRADE COMM'N Tr. at 8:2-8 (Mar. 13, 2001), https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.

[3] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal (Feb. 28, 2011), http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html [hereinafter *Web's New Hot Commodity*].

> may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[1]

66. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information.[2] The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

67. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349.[3]

68. The value of Plaintiffs and Class members' Private Information on the black market is substantial. Sensitive health information can sell for as much as $363.[4] This information is particularly valuable because criminals can use it to target victims with fraud and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

69. Medical identify theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

---

[1] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, FED. TRADE COMM'N (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

2 *Web's Hot New Commodity*, *supra* note 19.

3 *See* U.S. Dep't of Justice, *Victims of Identity Theft,* OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

[4] Center for Internet Security, *Data Breaches: In the Healthcare Sector*, https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/.

mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves their victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[1]

70. The ramifications of YRMC's failure to keep its patients' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

71. Approximately 21% of victims do not realize their identify has been compromised until more than two years after it has happened.[2] This gives thieves ample time to seek multiple treatments under the victim's name or perform other fraudulent acts with the stolen data. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[3]

72. Breaches are particularly serious in healthcare industries. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[4] Indeed, when compromised, healthcare related data is among the most private and personally consequential. A report focusing on healthcare breaches

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

[1] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, KAISER (Feb. 7, 2014) https://khn.org/news/rise-of-indentity-theft/.
[2] *See Medical ID Theft Checklist*, IDENTITYFORCE, https://www.identityforce.com/blog/medical-id-theft-checklist-2.
[3] *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches*, EXPERIAN, (Apr. 2010), https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.
[4] Identity Theft Resource Center, *2018 End-of-Year Data Breach Report*, (2019) https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

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.[1] Almost 50% of the surveyed victims lost their healthcare coverage as a result of the incident, while nearly 30% said their insurance premiums went up after the event. Forty percent of the victims were never able to resolve their identity theft at all. Seventy-four percent said that the effort to resolve the crime and restore their identity was significant or very significant. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[2]

73. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that the Private Information it maintains is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft and fraud. Defendant should have particularly been aware of these risks given the significant number of data breaches affecting the medical industry and related industries.

74. Had Defendant remedied the deficiencies in its security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Defendant would have prevented the ransomware attack into its systems and, ultimately, the theft of its patients' Private Information.

75. The compromised Private Information in the Data Breach is of great value to hackers and thieves and can be used in a variety of ways. Information about, or related to, an individual for which there is a possibility of logical association with other information is of great value to hackers and thieves. Indeed, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

[1] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for- victims/.
[2] *Id.*

constitute PII."[1] For example, different PII elements from various sources may be able to be linked in order to identify an individual, or access additional information about or relating to the individual.[2] Based upon information and belief, the unauthorized parties utilized the Private Information they obtained through the Data Breach to obtain additional information from Plaintiffs and Class members that was misused.

76. In addition, as technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

77. Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts. Thus, even if payment card information were not involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class members' Private Information to access accounts, including, but not limited to email accounts and financial accounts, to engage in the fraudulent activity identified by Plaintiffs.

78. Given these facts, any company that transacts business with customers and then compromises the privacy of their Private Information has thus deprived them of the full monetary value of their transaction with the company.

79. Acknowledging the damage to Plaintiffs and Class members, Defendant instructed patients to activate fraud alerts on the credit monitoring services provided by YRMC and remain vigilant. Plaintiffs and the other Class members now face a greater risk of identity theft.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

---

[1] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report*, FED. TRADE COMM'N 35-38 (Dec. 2010), https://www.ftc.gov/reports/preliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework.

[2] *See id.* (evaluating privacy framework for entities collecting or using consumer data with can be "reasonably linked to a specific consumer, computer, or other device").

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

80. In short, the Private Information exposed is of great value to hackers and cyber criminals and the data compromised in the Data Breaches can be used in a variety of unlawful manners, including opening new credit and financial accounts in users' names.

D. YRMC's Conduct violated HIPPA

81. HIPAA requires covered entities like YRMC to protect against reasonably anticipated threats to the security of PHI. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.[1]

82. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, et seq. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling Private Information like the data Defendant left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

83. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required Defendant to provide notice of the breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."[2]

84. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations. YRMC's security failures include, but are not limited to, the following:

- Failing to ensure the confidentiality and integrity of electronic protected health information that Defendant creates, receives, maintains, and transmits in violation of 45 C.F.R. §164.306(a)(1);

---

[1] *What is Considered Protected Health Information Under HIPAA*?, HIPPA JOURNAL, https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/.
[2] *Breach Notification Rule*, U.S. DEP'T HEALTH & HUMAN SERVS., https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

- Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health 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);

- 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);

- Failing to identify and respond to suspected or known security incidents; 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);

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

- Failing to protect against any reasonably anticipated uses or disclosures of electronically protected health 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);

- Failing to ensure compliance with HIPAA security standard rules by its workforce in violation of 45 C.F.R. §164.306(a)(94);

- Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 C.F.R. §164.502, *et seq.*;

- Failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out its functions and to maintain security of protected health information in violation of 45 C.F.R. §164.530(b) and 45 C.F.R. §164.308(a)(5); and

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

E. YRMC Failed to Comply with FTC Guidelines

85. YRMC was also prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

86. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[1]

87. In 2016, the FTC updated their publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses.[2] The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

88. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor

[1] *Start With Security: A Guide for Business*, FED. TRADE. COMM'N (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf [hereinafter *Start with Security*].

[2] *Protecting Personal Information: A Guide for Business*, FED. TRADE. COMM'M (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf- 0136_proteting-personal-information.pdf.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[1]

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

90. YRMC was at all times fully aware of its obligation to protect the Private Information of patients because of its position as a trusted healthcare provider. YRMC was also aware of the significant repercussions that would result from its failure to do so.

F. YRMC Failed to Comply with Healthcare Industry Standards

91. HHS's Office for Civil Rights has stated:

> While all organizations need to implement policies, procedures, and technical solutions to make it harder for hackers to gain access to their systems and data, this is especially important in the healthcare industry. Hackers are actively targeting healthcare organizations, as they store large quantities of highly Private and valuable data.[2]

92. HHS highlights several basic cybersecurity safeguards that can be implemented to improve cyber resilience that require a relatively small financial investment, yet can have a major impact on an organization's cybersecurity posture including: (a) the proper encryption of Private Information; (b) educating and training healthcare employees on how to protect Private Information; and (c) correcting the configuration of software and network devices.

93. Private cybersecurity firms have also identified the healthcare sector as being particularly vulnerable to cyber-attacks, both because the of value of the Private Information

[1] *Start with Security*, *supra* note 34.

[2] *Cybersecurity Best Practices for Healthcare Organizations*, HIPAA JOURNAL (Nov. 1, 2018), https://www.hipaajournal.com/important-cybersecurity-best-practices-for-healthcare-organizations/.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

which they maintain and because as an industry they have been slow to adapt and respond to cybersecurity threats.[1] They too have promulgated similar best practices for bolstering cybersecurity and protecting against the unauthorized disclosure of Private Information.

94. Despite the abundance and availability of information regarding cybersecurity best practices for the healthcare industry, YRMC chose to ignore them. These best practices were known, or should have been known by YRMC, whose failure to heed and properly implement them directly led to the Data Breach and the unlawful exposure of Private Information.

G. Damages to Plaintiffs and the Class

95. Plaintiffs and the Class have been damaged by the compromise of their Private Information in the Data Breach.

96. The ramifications of YRMC's failure to keep patients' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to the victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[2]

97. In addition to its obligations under state laws and regulations, Defendant owed a common law duty to Plaintiffs and Class members to protect Private Information entrusted to it, including to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized parties.

98. Defendant further owed and breached its duty to Plaintiffs and Class members to implement processes and specifications that would detect a breach of its security systems in a

[1] *See, e.g.*, *10 Best Practices For Healthcare Security*, INFOSEC, https://resources.infosecinstitute.com/topics/healthcare-information-security/#gref.
[2] *2014 LexisNexis True Cost of Fraud Study*, LEXISNEXIS (Aug. 2014), https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

99. As a direct result of Defendant's intentional, willful, reckless, and negligent conduct which resulted in the Data Breach, unauthorized parties were able to access, acquire, view, publicize, and/or otherwise cause the identity theft and misuse to Plaintiffs' and Class members' Private Information as detailed above, and Plaintiffs are now at a heightened and increased risk of identity theft and fraud.

100. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

101. Some of the risks associated with the loss of their Private Information have already manifested themselves in Plaintiffs' case. Plaintiffs received a cryptically written notice letter from Defendant stating that their Private Information was released, where it may have gone, or who could have had access to it. Plaintiffs and Class members have already experienced misuse of their Private Information and spent hours dealing with the negative effects of the Data Breach and trying to determine what additional negative effects may occur from the loss of their Private Information.

102. Indeed, the risk of unauthorized actors misusing Plaintiffs' Private Information is not just theoretical in this case. Plaintiff Ashby was notified that her Private Information, some of which was disclosed in the Data Breach, was used to file a tax return in her name with the IRS.

103. By entrusting their Private Information to Defendant, Plaintiffs and Class members released information that they had a property interest in and entrusted Defendant with

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

the responsibility of avoiding its negligent release to unauthorized third parties. Defendant failed to fulfill its role in this agreement.

104. Plaintiffs and the Class have suffered and/or face a substantial risk of suffering out-of-pocket fraud losses such as fraudulent charges on online accounts, tax returns filed in their names, credit card fraud, loans opened in their names, medical services billed in their name, and similar identity theft.

105. Plaintiffs and Class members have, may have, and/or will have incurred out of pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

106. Plaintiffs and Class members did not receive the full benefit of the bargain made with Defendant and instead received services that were of a diminished value to that described in their agreements with YRMC. They were damaged in an amount at least equal to the difference in the value of the services with data security protection they paid for and the services they received.

107. Plaintiffs and Class members would not have obtained services from Defendant had Defendant told them that it failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard its Private Information from theft.

108. Plaintiffs and the Class will continue to spend significant amounts of time to monitor their financial and medical accounts for misuse.

109. The theft of Social Security Numbers, which were purloined as part of the Data Breach, is particularly detrimental to victims. The U.S. Social Security Administration ("SSA") warns that "[i]dentity theft is one of the fastest growing crimes in America."[1] The SSA has stated that "[i]dentity thieves can use your number and your good credit to apply for more credit

1 *Identity Theft And Your Social Security Number*, SOCIAL SECURITY ADMIN. (Dec. 2013), http://www.ssa.gov/pubs/EN-05-10064.pdf.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought."[1] In short, "[s]omeone illegally using your Social Security number and assuming your identity can cause a lot of problems."[2]

110. In fact, a new Social Security number is substantially less effective where "other personal information, such as [the victim's] name and address, remains the same" and for some victims, "a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under your new number may make it more difficult for you to get credit."[3]

111. Identity thieves can use the victims' Private Information to commit any number of frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest. In the healthcare industry context, Private Information can be used to submit false insurance claims. As a result, Plaintiffs and Class members now face a real and continuing immediate risk of identity theft and other problems associated with the disclosure of their Social Security numbers, and will need to monitor their credit for an indefinite duration. For Plaintiffs and Class members, this risk creates unending feelings of fear and annoyance. Private information is especially valuable to identity thieves. Defendant knew or should have known this and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

112. As a result of the Data Breach, Plaintiffs' and Class members' Private Information has diminished in value.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

[1] *Id.*
[2] *Id.*
[3] *Id.*

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

113. The Private Information belonging to Plaintiffs and Class members is private in nature, and was left inadequately protected by Defendant who did not obtain Plaintiffs' or Class members' consent to disclose such Private Information to any other person as required by applicable law and industry standards. Defendant disclosed information about Plaintiffs and the Class that was of an extremely personal, sensitive nature as a direct result of its inadequate security measures.

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

115. Defendant had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite its obligation to protect patient data.

116. Defendant did not properly train its employees to identify and avoid ransomware attacks.

117. Had Defendant remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field, they would have prevented the intrusions into its systems and, ultimately, the theft of Plaintiffs' and Class members' Private Information.

118. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiffs and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

119. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, twenty-nine percent spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[1]

120. Other than offering 12 months of credit monitoring, Defendant did not take any measures to assist Plaintiffs and Class members other than telling them to simply do the following:

- remain vigilant for incidents of fraud and identity theft;
- review account statements and monitor credit reports for unauthorized activity;
- obtain a copy of free credit reports;
- contact the FTC and/or the state Attorney General's office;
- enact a security freeze on credit files; and
- create a fraud alert.

None of these recommendations, however, require Defendant to expend any effort to protect Plaintiffs and Class members' Private Information.

121. Defendant's failure to adequately protect Plaintiffs and Class members' Private Information has resulted in Plaintiffs and Class members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money–while Defendant sits by and does nothing to assist those affected by the incident. Instead, as YRMC's Data Breach Notice indicates, it is putting the burden on Plaintiffs and Class members to discover possible fraudulent activity and identity theft.

---

[1] *See* U.S. Dep't of Justice, *Victims of Identity Theft,* OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

122. While Defendant offered one year of free credit monitoring, Plaintiffs would rather not trust a company that had already lost their highly sensitive data before ensuring that it has taken meaningful steps in improving its data security practices.

123. Moreover, the offer of 12 months of identity monitoring to Plaintiffs and Class members is woefully inadequate. While some harm has begun already, the worst may be yet to come. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is acquired and when it is used. Furthermore, identity monitoring only alerts someone to the fact that they have already been the victim of identity theft (i.e., fraudulent acquisition and use of another person's Private Information) – it does not prevent identity theft.[1] This is especially true for many kinds of medical identity theft, for which most credit monitoring plans provide little or no monitoring or protection.

124. Plaintiffs and Class members have been damaged in several other ways as well. Plaintiffs and Class members have been exposed to an impending, imminent, and ongoing increased risk of fraud, identity theft, and other misuse of their Private Information. Plaintiffs and Class members must now and indefinitely closely monitor their financial and other accounts to guard against fraud. This is a burdensome and time-consuming activity. Plaintiffs and Class members have also purchased credit monitoring and other identity protection services, purchased credit reports, placed credit freezes and fraud alerts on their credit reports, and spent time investigating and disputing fraudulent or suspicious activity on their accounts. Plaintiffs and Class members also suffered a loss of the inherent value of their Private Information.

125. The Private Information stolen in the Data Breach can be misused on its own, or can be combined with personal information from other sources such as publicly available information, social media, etc. to create a package of information capable of being used to

[1] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, CNBC (Nov. 30, 2017), https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-beworth-the-cost.html.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

commit further identity theft. Thieves can also use the stolen Private Information to send spear-phishing emails to Class members to trick them into revealing sensitive information. Lulled by a false sense of trust and familiarity from a seemingly valid sender (for example Wells Fargo, Amazon, or a government entity), the individual agrees to provide sensitive information requested in the email, such as login credentials, account numbers, and the like.

126. As a result of Defendant's failures to prevent the Data Breach, Plaintiffs and Class members have suffered, will suffer, and are at increased risk of suffering:

- The compromise, publication, theft and/or unauthorized use of their Private Information;
- Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;
- Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from 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;
- 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 appropriate measures to protect the Private Information in its possession;
- Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class members; and
- Anxiety and distress resulting fear of misuse of their Private Information.

127. In addition to a remedy for the economic harm, Plaintiffs and Class members maintain an undeniable interest in ensuring that their Private Information remains secure and is not subject to further misappropriation and theft.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

CLASS ACTION ALLEGATIONS

128. Plaintiffs incorporate by reference all other paragraphs of this Complaint as if fully set forth herein.

129. Plaintiffs bring this action individually and on behalf of a "Nationwide Class" and "Arizona Subclass" of persons similarly situated (collectively, the "Class") pursuant to Rule 23 of the Arizona Rules of Civil Procedure.

130. Plaintiffs propose the following Class definitions subject to amendment based on information obtained through discovery. Notwithstanding, at this time, Plaintiffs brings this action and seek certification of the following Nationwide Class and Arizona Subclass:

Nationwide Class

All persons whose Private Information was compromised as a result of the Data Breach discovered on or about April of 2022 and who were sent notice of the Data Breach.

Arizona Subclass

All persons residing in Arizona whose Private Information was compromised as a result of the Data Breach discovered on or about April of 2022 and who were sent notice of the Data Breach.

Excluded from the Class are Defendant and Defendant's affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

131. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

132. **Numerosity—Fed. R. Civ. P. 23(a)(1).** The members of the Class are so numerous that joinder of all Class members would be impracticable. On information and belief, the Nationwide Class numbers in the tens of thousands.

133. **Commonality and Predominance—Fed. R. Civ. P. 23(a)(2).** Common questions of law and fact exist as to all members of the Class and predominate over questions affecting only individual members of the Class. Such common questions of law or fact include, *inter alia*:

- Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;
- Whether Defendant properly implemented its purported security measures to protect Plaintiffs' and the Class's Private Information from unauthorized capture, dissemination, and misuse;
- Whether Defendant took reasonable measures to determine the extent of the Data Breach after it first learned of same;
- Whether Defendant disclosed Plaintiffs' and the Class's Private Information in violation of the understanding that the Private Information was being disclosed in confidence and should be maintained;
- Whether Defendant willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiffs' and the Class's Private Information;
- Whether Defendant was negligent in failing to properly secure and protect Plaintiffs' and the Class's Private Information;
- Whether Defendant was unjustly enriched by its actions; and
- Whether Plaintiffs and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

134. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of themselves and other members of the Class. Similar or identical common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

135. **Typicality—Fed. R. Civ. P. 23(a)(3).** Plaintiffs' claims are typical of the claims of the other members of the Class because, among other things, all Class members were similarly injured through Defendant's uniform misconduct described above and were thus all subject to the Data Breach alleged herein. Further, there are no defenses available to Defendant that are unique to Plaintiffs.

136. **Adequacy of Representation—Fed. R. Civ. P. 23(a)(4).** Plaintiffs are adequate representatives of the Nationwide Class because their interests do not conflict with the interests of the Classes they seek to represent, they have retained counsel competent and experienced in complex class action litigation, and Plaintiffs will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiffs and their counsel.

137. **Superiority—Fed. R. Civ. P. 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and the other members of the Class are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for members of the Class to individually seek redress for Defendant's wrongful conduct. Even if members of the Class could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

management difficulties and provides the benefit of a single adjudication, economy of scale, and comprehensive supervision by a single court.

COUNT I
Negligence
(On Behalf of the Nationwide Class, or in the alternative, the Arizona Subclass)

138. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

139. Upon Defendant's accepting and storing the Private Information of Plaintiffs and the Class in their computer systems and on their networks, Defendant undertook and owed a duty to Plaintiffs and the Class to exercise reasonable care to secure and safeguard that Information and to use commercially reasonable methods to do so. Defendant knew that the Private Information was private and confidential and should be protected as private and confidential.

140. Defendant owed a duty of care not to subject Plaintiffs' and the Class's Private Information to an unreasonable risk of exposure and theft because Plaintiffs and the Class were foreseeable and probable victims of any inadequate security practices.

141. Defendant owed numerous duties to Plaintiffs and the Class, including the following:

- to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private Information in their possession;
- to protect Private Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and
- to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

142. Defendant also breached its duty to Plaintiffs and Class members to adequately protect and safeguard Private Information by disregarding standard information security

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information. Furthering its dilatory practices, Defendant failed to provide adequate supervision and oversight of the Private Information with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a malicious third party to gather Plaintiffs' and Class members' Private Information and potentially misuse the Private Information and intentionally disclose it to others without consent.

143. Defendant knew, or should have known, of the risks inherent in collecting and storing Private Information and the importance of adequate security. Defendant knew or should have known about numerous well-publicized data breaches within the medical industry.

144. Defendant knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiffs' and Class members' Private Information.

145. Defendant breached its duties to Plaintiffs and Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' Private Information.

146. Because Defendant knew that a breach of their systems would damage thousands of its patients, including Plaintiffs and Class members, Defendant had a duty to adequately protect its data systems and the Private Information contained thereon.

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

148. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . .

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

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.

149. Defendant also had a duty under HIPAA privacy laws, which were enacted with the objective of protecting the confidentiality of clients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

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

151. Defendant's own conduct also created a foreseeable risk of harm to Plaintiffs and Class members and their Private Information. Defendant's misconduct included failing to: (1) secure Plaintiffs' and Class member's Private Information; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

152. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class members' Private Information, and by failing to provide timely notice of the Data Breach. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- Failing to adopt, implement, and maintain adequate security measures to safeguard Class members' Private Information;
- Failing to adequately monitor the security of Defendant's networks and systems;
- Allowing unauthorized access to Class members' Private Information;

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

- Failing to detect in a timely manner that Class members' Private Information had been compromised; and

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

153. Through Defendant's acts and omissions described in this Complaint, including its failure to provide adequate security and failure to protect Plaintiffs' and Class members' Private Information from being foreseeably captured, accessed, disseminated, stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiffs' and Class members' Private Information during the time it was within Defendant's possession or control.

154. Defendant's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to failing to adequately protect the Private Information and failing to provide Plaintiffs and Class members with timely notice that their sensitive Private Information had been compromised.

155. Neither Plaintiffs nor the other Class members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

156. As a direct and proximate cause of Defendant's conduct, Plaintiffs and Class members suffered damages as alleged above.

157. Plaintiffs and Class members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen data security systems and monitoring procedures; (ii) submit to future annual audit of those systems and monitoring procedures; and (iii) immediately provide free lifetime credit monitoring to all Class members.

COUNT II
Breach of Contract

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

(On Behalf of the Nationwide Class, or in the alternative, the Arizona Subclass)

158. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

159. Plaintiffs and other Class members entered into valid and enforceable express contracts with Defendant under which Plaintiffs and other Class members agreed to provide their Private Information to Defendant, and Defendant agreed to provide health services and, impliedly, if not explicitly, agreed to protect Plaintiffs' and Class members' Private Information.

160. These contracts include HIPAA privacy notices and explanation of benefit documents.

161. To the extent Defendant's obligation to protect Plaintiffs' and other Class members' Private Information was not explicit in those express contracts, the express contracts included implied terms requiring Defendant to implement data security adequate to safeguard and protect the confidentiality of Plaintiffs' and other Class members' Private Information, including in accordance with HIPAA regulations; federal, state and local laws; and industry standards. Plaintiffs and Class members would not have entered into these contracts with Defendant without the understanding that their Private Information would be safeguarded and protected; stated otherwise, data security was an essential implied term of the parties' express contracts.

162. A meeting of the minds occurred, as Plaintiffs and Class members agreed, among other things, to provide their Private Information in exchange for Defendant's agreement to protect the confidentiality of that Private Information.

163. The protection of Plaintiffs' and Class members' Private Information was a material aspect of Plaintiffs' and Class members' contracts with Defendant.

164. Defendant's promises and representations described above relating to HIPAA and industry practices and Defendant's purported concern about its clients' privacy rights became terms of the contracts between Defendant and its clients, including Plaintiffs and Class

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

members. Defendant breached these promises by failing to comply with HIPAA and reasonable industry practices.

165. Plaintiffs and Class members read, reviewed, and/or relied on statements made by or provided by YRMC and/or otherwise understood that YRMC would protect its patients' Private Information if that information were provided to YRMC.

166. Plaintiffs and Class members fully performed their obligations under the implied contract with Defendant; however, Defendant did not.

167. As a result of Defendant's breach of these terms, Plaintiffs and Class members have suffered a variety of damages including but not limited to: the lost value of their privacy; they did not get the benefit of their bargain with Defendant; they lost the difference in the value of the secure health services Defendant promised and the insecure services received; the value of the lost time and effort required to mitigate the actual and potential impact of the Data Breach on their lives, including, inter alia, that required to place "freezes" and "alerts" with credit reporting agencies, to contact financial institutions, to close or modify financial and medical accounts, to closely review and monitor credit reports and various accounts for unauthorized activity, and to file police reports; and Plaintiffs and other Class members have been put at increased risk of future identity theft, fraud, and/or misuse of their Private Information, which may take years to manifest, discover, and detect.

168. Plaintiffs and Class members are therefore entitled to damages, including restitution and unjust enrichment, disgorgement, declaratory and injunctive relief, and attorney fees, costs, and expenses.

COUNT III
Breach of Implied Contract
(On Behalf of the Nationwide Class, or in the alternative, the Arizona Subclass)

169. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

170. Through its course of conduct, Defendant entered into implied contracts with Plaintiffs and Class members for the provision of healthcare services, as well as implied contracts requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class members' Private Information.

171. Specifically, Plaintiffs and Class members entered into a valid and enforceable implied contract with Defendant when they first entered into the health services agreement with Defendant.

172. The valid and enforceable implied contracts to provide health services that Plaintiffs and Class members entered into with Defendant include Defendant's promise to protect nonpublic Private Information given to Defendant or that Defendant creates on its own from disclosure.

173. When Plaintiffs and Class members provided their Private Information to Defendant in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such Information.

174. Defendant solicited and invited Plaintiffs and Class members to provide their Private Information as part of Defendant's regular business practices. Plaintiffs and Class members accepted Defendant's offers and provided their Private Information to Defendant.

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

176. Class members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

177. Under these implied contracts, Defendant and/or its affiliated providers promised and were obligated to: (a) provide healthcare services to Plaintiffs and Class members; and (b) protect Plaintiffs' and the Class members' Private Information provided to obtain such benefit

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

of such services. In exchange, Plaintiffs and members of the Class agreed to pay money for these services, and to turn over their Private Information to Defendant.

178. Both the provision of health services and the protection of Plaintiffs' and Class members' Private Information were material aspects of these implied contracts.

179. The implied contracts for the provision of healthcare services—contracts that include the contractual obligations to maintain the privacy of Plaintiffs' and Class members' Private Information—are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendant's Data Breach notification letter.

180. Defendant's express representations, including, but not limited to the express representations found in its Privacy Notice, memorialize and embody the implied contractual obligations requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and protect the privacy of Plaintiffs' and Class members Private Information.

181. Consumers of health services value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining such services. Plaintiffs and Class members would not have entrusted their Private Information to Defendant and entered into these implied contracts with Defendant without an understanding that their Private Information would be safeguarded and protected; nor would Plaintiffs or Class members have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

182. A meeting of the minds occurred, as Plaintiffs and Class members agreed and provided their Private Information to Defendant and/or its affiliated healthcare providers and paid for the provided health services in exchange for, amongst other things, both the provision of healthcare and the protection of their Private Information.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

183. Plaintiffs and Class members performed their obligations under the contract when they paid for Defendant's services and provided their Private Information.

184. Defendant materially breached its contractual obligation to protect the nonpublic Private Information Defendant gathered when the information was accessed and exfiltrated by the Data Breach.

185. Defendant materially breached the terms of the implied contracts, including, but not limited to, the terms stated in the relevant Notice of Privacy Practices. Defendant did not maintain the privacy of Plaintiffs' and Class members' Private Information as evidenced by its notifications of the Data Breach to Plaintiffs and Class members. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like Section 5 of the FTCA, or otherwise protect Plaintiffs' and Class members' private information as set forth above.

186. The Data Breach was a reasonably foreseeable consequence of Defendant's action in breach of these contracts.

187. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiffs and Class members did not receive full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in the contracts. Plaintiffs and Class members therefore were damaged in an amount at least equal to the difference in the value of the healthcare with data security protection they paid for and the healthcare they received.

188. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiffs, Class members, nor any reasonable person would have purchased healthcare from Defendant and/or its affiliated providers.

189. As a direct and proximate result of the Data Breach, Plaintiffs and Class members have been harmed and suffered, and will continue to suffer, actual damages and injuries,

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out of pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

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

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

COUNT IV
Breach of Fiduciary Duty
(On Behalf of the Nationwide Class, or in the alternative, the Arizona Subclass)

192. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

193. In providing their Private Information to Defendant, Plaintiffs and Class members justifiably placed a special confidence in Defendant to act in good faith and with due regard to interests of Plaintiffs and Class members to safeguard and keep confidential that Private Information.

194. Defendant accepted the special confidence Plaintiffs and Class members placed in it, as evidenced by its assertion that it is "committed to protecting the privacy of [Plaintiffs'] personal information" as included in the Data Breach notification letter.

195. In light of the special relationship between Defendant and Plaintiffs and Class members, whereby Defendant became a guardian of Plaintiffs' and Class members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its patients, including Plaintiffs and Class members for the safeguarding of Plaintiffs' and Class members' Private Information.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

196. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of its patients' relationship, in particular, to keep secure the Private Information of its patients.

197. Defendant breached its fiduciary duties to Plaintiffs and Class members by failing to protect the integrity of the systems containing Plaintiffs' and Class member's Private Information.

198. Defendant breached its fiduciary duties to Plaintiffs and Class members by otherwise failing to safeguard Plaintiffs' and Class members' Private Information.

199. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class members; and (vii) the diminished value of Defendant's services they received.

200. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT V

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

Unjust Enrichment
(On Behalf of the Nationwide Class, or in the alternative, the Arizona Subclass)

201. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

202. This claim is pleaded only in the alternative to Plaintiff's express and implied contract claims.

203. Plaintiffs and Class members conferred a monetary benefit upon YRMC in the form of monies paid for healthcare services at its locations

204. YRMC appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and Class members.

205. YRMC also benefitted from the receipt of Plaintiffs' and Class members' Private Information, as this was used to facilitate payment and to make insurance claims.

206. As a result of YRMC's conduct, Plaintiffs and Class members suffered actual damages in an amount equal to the difference in value between their purchases made with reasonable data privacy and security practices and procedures that Plaintiffs and Class members paid for, and those purchases without unreasonable data privacy and security practices and procedures they received.

207. Under principles of equity, YRMC should not be permitted to retain the money belonging to Plaintiffs and Class members because YRMC failed to implement (or adequately implement) the data privacy and security practices and procedures for which Plaintiffs and Class members paid, and which were otherwise mandated by federal, state, and local laws and by industry standard.

208. YRMC should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class members all unlawful or inequitable proceeds it received as a result of its conduct and the Data Breach incident.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

COUNT VI
Violation of the Arizona Consumer Fraud Act
Ariz. Rev. Stat. § 44-1522 *et seq.*
(On Behalf of the Arizona Subclass)

209. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

210. Plaintiffs, and the Arizona Subclass members were engaged in transactions and conduct to procure services in connection with Defendant.

211. Defendant engaged in transactions and conduct to procure services on behalf of Plaintiffs and Arizona Subclass members as defined by Ariz. Rev. Stat. § 44- 1521(5).

212. Defendant engaged in trade and commerce through its acts and omissions and its course of business, including promises that it would maintain its patients' information.

213. As alleged herein in this Complaint, Defendant engaged in unfair or deceptive acts or practices in the conduct of consumer transactions in violations of the Arizona Consumer Fraud Act, including but not limited to:

- Representing that its services were of a particular standard or quality that it knew or should have known were of another;
- Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Arizona Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;
- Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;
- Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

- Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Arizona Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

- Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Arizona Subclass members' Private Information; and

- Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Arizona Subclass members' Private Information Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Security breach.

214. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Private Information.

215. In addition, Defendant's failure to secure patients' Private Information violated the FTCA and therefore violates the Consumer Fraud Act.

216. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the Private Information of Plaintiffs and Arizona Subclass members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

217. The aforesaid conduct violated the Consumer Fraud Act, Ariz. Rev. Stat. § 44-1521(5) *et seq.*, in that it is a restraint on trade or commerce.

218. The Defendant's violations of the Consumer Fraud Act have an impact of great and general importance to the public, including the people of Arizona. Thousands of Arizona residents have been treated by YRMC, many of whom have been impacted by the Data Breach. In addition, Arizona residents have a strong interest in regulating the conduct of its hospitals, whose policies described herein affect millions of people across the country.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

219. As a direct and proximate result of Defendant's violation of the Consumer Fraud Act, Plaintiffs and Arizona Subclass members are entitled to judgment under Ariz. Rev. Stat. § 44- 1521(5), *et seq.*, to enjoin further violations, to recover actual damages, to recover the costs of this action (including reasonable attorney's fees), and such other further relief as the Court deems just and proper.

220. On information and belief, YRMC formulated and conceived of the systems it used to compile and maintain patient information largely within the state of Arizona, oversaw its data privacy program complained herein from Arizona, and its communications and other efforts to hold patient data largely emanated from Arizona.

221. Most, if not all, of the alleged misrepresentations and omissions by YRMC that led to inadequate safety measures to protect patient information occurred within or were approved within Arizona.

222. Defendant's implied and express representations that they would adequately safeguard Plaintiffs' and Arizona Subclass members' Private Information constitute representations as to the particular standard, quality, or grade of services that such services did not actually have (as the data security services were of another, inferior quality), in violation of Ariz. Rev. Stat. § 44- 1521(5), *et seq.*

223. These violations have cause financial injury to Plaintiffs and Arizona Subclass members and created an unreasonable, imminent risk of future injury.

224. Accordingly, Plaintiffs, on behalf of themselves and Arizona Subclass members, bring this action under the Deceptive Consumer Sales Act to seek such injunctive relief necessary to enjoin further violations and to recover costs of this action, including reasonable attorney's fees and other costs.

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

COUNT VII
Declaratory Relief
(On Behalf of the Nationwide Class, or in the alternative, the Arizona Subclass)

225. Plaintiffs fully incorporate by reference all of the above paragraphs as though fully set forth herein.

226. Under the Arizona Declaratory Judgment Act, Ariz. Rev. Stat. § 12-1831, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

227. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard Plaintiffs' and Class members' Private Information, and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class members from further data breaches that compromise their Private Information. Plaintiffs and the Class remain at imminent risk that further compromises of their Private Information will occur in the future.

228. The Court should also issue prospective injunctive relief requiring Defendant to employ adequate security practices consistent with law and industry standards to protect consumer and patient Private Information.

229. Defendant still possesses the Private Information of Plaintiffs and the Class.

230. Defendant has made no announcement that it has changed its data storage or security practices relating to the Private Information.

231. Defendant has made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

232. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at YRMC. The risk of another such breach is real, immediate, and substantial.

233. The hardship to Plaintiffs and Class members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another data breach occurs at YRMC, Plaintiffs and Class members will likely continue to be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

234. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at YRMC, thus eliminating the additional injuries that would result to Plaintiffs and Class members, along with other patients whose Private Information would be further compromised.

235. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that YRMC implement and maintain reasonable security measures, including but not limited to the following:

- Engaging third-party security auditors/penetration testers, as well as internal security personnel, to conduct testing that includes simulated attacks, penetration tests, and audits on YRMC's systems on a periodic basis, and ordering YRMC to promptly correct any problems or issues detected by such third-party security auditors;
- engaging third-party security auditors and internal personnel to run automated security monitoring;
- auditing, testing, and training its security personnel regarding any new or modified procedures;

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

- purging, deleting, and destroying Private Information not necessary for its provisions of services in a reasonably secure manner;
- conducting regular database scans and security checks; and
- routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Defendant, as follows:

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

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

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

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

E. Ordering Defendant to pay for not less than three (3) years of credit monitoring services for Plaintiffs and the Classes;

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

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

PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301

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

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

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

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

RESPECTFULLY SUBMITTED this 21st day of July, 2022.

/s/ Cristina Perez Hesano
Cristina Perez Hesano (#027023)
PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301
Telephone: (602) 730-7100
Fax: (602) 794-6956
cperez@perezlawgroup.com

/s/ Nicholas A. Migliaccio
Nicholas A. Migliaccio (pro hac vice anticipated)
nmigliaccio@classlawdc.com
Jason S. Rathod (pro hac vice anticipated)
jrathod@*classlawdc.com*
Tyler Bean (pro hac vice anticipated)
Kevin Leddy (pro hac vice anticipated)
Migliaccio & Rathod LLP
412 H Street NE
Washington, DC 20002
Tel: (202) 470-3520
Fax: (202 800-2730

Counsel for Plaintiffs