Exhibit A

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

Daniel O. Herrera, IL SBN (6296731), *pro hac vice pending*
Nickolas J. Hagman, IL SBN (6317689), *pro hac vice pending*
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
135 S. LaSalle, Suite 3210
Chicago, Illinois 60603
Telephone: (312) 782-4880
Facsimile: (312) 782-4485
dherrera@caffertyclobes.com
nhagman@caffertyclobes.com

Attorneys for Plaintiffs and the Proposed Class

IN THE SUPERIOR COURT OF THE STATE OF ARIZONA

IN AND FOR THE COUNTY OF MARICOPA

MICHELE STROUP and GEORGIOS ASIMAKOPOULOS, individually, and on behalf of all others similarly situated, Plaintiffs, v. CARDIOVASCULAR CONSULTANTS, LTD., Defendant.	Case No.: CV2023-020048 **CLASS ACTION COMPLAINT** **CLASS REPRESENTATION** (Jury Trial Requested)

Plaintiffs Michele Stroup and Georgios Asimakopoulos ("Plaintiffs"), individually, and on behalf of all others similarly situated, bring this action against the Cardiovascular

Consultants, Ltd. ("CVC" or "Defendant"). Plaintiffs bring this action by and through their attorneys, and allege, based upon personal knowledge as to their own actions, and based upon information and belief and reasonable investigation by their counsel as to all other matters, as follows.

INTRODUCTION

1. Cardiovascular Consultants, Ltd. is a healthcare services company that provides outpatient rehabilitation services.

2. As part of its operations, CVC collects, maintains, and stores highly sensitive personal and medical information belonging to its patients, and patients' financial guarantors, including, but not limited to: names, addresses, Social Security numbers, dates of birth, demographic and contact information, email addresses, driver's license numbers ("personally identifying information" or "PII"), information regarding insurance policies and guarantors, diagnosis and treatment, and medical and billing records ("private health information" or "PHI") (collectively, "Private Information").

3. Sometime on or before September 27, 2023, Defendant experienced a data breach incident in which unauthorized cybercriminals accessed its information systems and databases and stole Private Information belonging to Defendant's patients and patients' financial guarantors, including Plaintiffs and Class members. Defendant did not discover this breach until September 29, 2023. This investigation determined that various categories of information maintained by CVC was compromised in the breach. The following types of information belonging to patients was compromised: name, mailing address, date of birth, demographic and contact information, emergency contact information, Social Security number, driver's license and state ID numbers, insurance policy and guarantor information, diagnosis and treatment information, and other information from medical and billing records. The following types of information belonging to financial guarantors were compromised: name, date of birth, email address, telephone number, and mailing address. And the following types of information

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

belonging to policy holder/insurance subscribers were compromised: name, mailing address, telephone number, date of birth, Social Security number, and insurance information.

4. On December 2, 2023, Defendant sent notice to the individuals whose information was accessed in this incident.

5. Because Defendant stored and handled the highly-sensitive Private Information, it had a duty and obligation to safeguard this information and prevent unauthorized third parties from accessing this data.

6. Defendant failed to fulfill this obligation as unauthorized cybercriminals breached Defendant's information systems and databases, and stole vast quantities of Private Information belonging to Defendant's patients and patients' guarantors, including Plaintiffs and Class members. This breach and the successful exfiltration of Private Information were direct, proximate, and foreseeable results of multiple failings on the part of Defendant.

7. The data breach occurred because Defendant failed to implement reasonable security protections to safeguard its information systems and databases. Further, Defendant failed to inform the public that its data security practices were deficient and inadequate.

8. Defendant's subsequent handling of the breach was also deficient: Defendant failed to timely detect in a the data breach; and failed to inform Plaintiffs and Class members in a timely manner that their Private Information was stolen, delaying sending notice until 64 days after Defendant discovered the breach.

9. As a result of Defendant's negligent, reckless, intentional, and/or unconscionable failure to adequately satisfy its contractual, statutory, and common-law obligations, Plaintiffs and Class members suffered injuries as a result of Defendant's conduct including, but not limited to:

- Lost or diminished value of their Private Information;
- Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information;

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

- Lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges;

- Time needed to change usernames and passwords on their accounts;

- Time needed to investigate, correct and resolve unauthorized access to their accounts; time needed to deal with spam messages and e-mails received subsequent to the Data Breach;

- Charges and fees associated with fraudulent charges on their accounts; and the continued and increased risk of compromise 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 their Private Information.

10. Accordingly, Plaintiffs bring this action on behalf of all those similarly situated to seek relief for the consequences of Defendant's failure to reasonably safeguard Plaintiffs' and Class members' Private Information; Defendant's failure to reasonably provide timely notification to Plaintiffs and Class members that their Private Information had been compromised; and for Defendant's failure to inform Plaintiffs and Class members concerning the status, safety, location, access, and protection of their Private Information.

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

PARTIES

Plaintiff Michele Stroup

11. Plaintiff Stroup is a resident and citizen of Peoria, Arizona. Plaintiff Stroup was a patient of CVC. Plaintiff Stroup received Defendant's Data Breach Notice.

Plaintiff Georgios Asimakopoulos

12. Plaintiff Asimakopoulos is a resident and citizen of Scottsdale, Arizona. Plaintiff Asimakopoulos was a patient of CVC. Plaintiff Asimakopoulos received Defendant's Data Breach Notice.

Defendant Cardiovascular Consultants, Ltd.

13. Defendant Cardiovascular Consultants is an Arizona corporation with its principal place of business located at 3800 N Central Ave, Ste. 460, Phoenix, AZ 85012, USA. Defendant is specialist healthcare services provider that serves patients throughout Arizona.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this action because it is a court of general jurisdiction.

15. This Court has personal jurisdiction over Defendant because Defendant is a domestic corporation with its principal place of business in Arizona.

16. Venue is proper in this District pursuant to A.R.S. § 12-401 because Defendant is headquartered in this district.

FACTUAL ALLEGATIONS

A. Cardiovascular Consultants – Background

17. Defendant is a specialist healthcare services provider that operates throughout Arizona. As part of its operations, it collects the following types of information from its patients: name, mailing address, date of birth, demographic and contact information, emergency contact information, Social Security number, driver's license and state ID numbers, insurance policy and guarantor information, diagnosis and treatment information, and other information from medical and billing records. CVC stores this collected information on its databases.

18. On information and belief, CVC had failed to implement necessary data security safeguards at the time of the Data Breach. This failure resulted in cybercriminals accessing the Private Information of CVC's current and former patients and patients' guarantors—Plaintiffs and Class Members.

19. Current and former patients of CVC and their guarantors, such as Plaintiffs and Class Members, made their Private Information available to CVC with the reasonable expectation that any entity with access to this information would keep that sensitive and

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

personal information confidential and secure from illegal and unauthorized access. And, in the event of any unauthorized access, these entities would provide them with prompt and accurate notice.

20. This expectation was objectively reasonable and based on an obligation imposed on CVC by statute, regulations, industrial custom, and standards of general due care.

21. Unfortunately for Plaintiffs and Class Members, CVC failed to carry out its duty to safeguard sensitive Private Information and provide adequate data security. As a result, it failed to protect Plaintiffs and Class members from having their Private Information accessed and stolen during the Data Breach.

B. <u>The Data Breach</u>

22. On or before September 27, 2023, cybercriminals breached and accessed CVC's systems.

23. On September 29, 2023, CVC discovered the intrusion and began an investigation.

24. CVC maintained large volumes of information as part of its operations. CVC collected and stored the following types of information from its patients: name, mailing address, date of birth, demographic and contact information, emergency contact information, Social Security number, driver's license and state ID numbers, insurance policy and guarantor information, diagnosis and treatment information, and other information from medical and billing records. CVC collected and stored the following types of information belonging to financial guarantors were compromised: name, date of birth, email address, telephone number, and mailing address. And CVC collected and stored the following types of information belonging to policy holder/insurance subscribers were compromised: name, mailing address, telephone number, date of birth, Social Security number, and insurance information.

25. While the complete scope of the breach is not clear, it is probable that cybercriminals were able to access and exfiltrate a large proportion of this stored information.

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

26. On December 2, 2023, CVC sent out a data breach notice to all individuals it believed was affected by this data security incident.

C. CVC's Many Failures Both Prior to and Following the Breach

27. Defendant collects and maintains vast quantities of Private Information belonging to Plaintiffs and Class members as part of its normal operations as a healthcare service provider. The data breach occurred as direct, proximate, and foreseeable results of multiple failings on the part of Defendant.

28. First, Defendant failed to implement reasonable security protections to safeguard its information systems and databases.

29. Second, Defendant failed to inform the public that its data security practices were deficient and inadequate. Had Plaintiffs and Class members been aware that Defendant did not have adequate safeguards in place to protect such sensitive Private Information, they would have never provided such information to Defendant.

30. In addition to the failures that lead to the successful breach, Defendant's failings in handling the breach and responding to the incident exacerbated the resulting harm to Plaintiffs and the Class.

31. Defendant failed to timely inform Plaintiffs and Class members that their information was stolen, waiting until 64 days after it detected the data breach to finally provide notice to affected individuals. This delay virtually ensured that the cybercriminals who stole Private Information could monetize, misuse and/or disseminate that Private Information before Plaintiffs and Class members could take affirmative steps to protect themselves. As a result, Plaintiffs and Class members will suffer indefinitely from the substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated.

32. Additionally, Defendant's attempt to ameliorate the effects of this data breach with 2-years of complimentary credit monitoring is inadequate. Plaintiffs' and Class members' Private Information was accessed and acquired by cybercriminals for the express purpose of misusing the data. As a consequence, they face the real, immediate, and likely danger of identity

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

theft and misuse of their Private Information. And this can, and in some circumstances already has, caused irreparable harm to their personal, financial, reputational, and future well-being. This harm is even more acute because much of the stolen Private Information, such as healthcare data, is immutable.

33. In short, Defendant's myriad failures, including the failure to timely detect an intrusion and failure to timely notify Plaintiffs and Class members that their personal and medical information had been stolen due to Defendant's security failures, allowed unauthorized individuals to access, misappropriate, and misuse Plaintiffs' and Class members' Private Information for 64 days before Defendant finally granted victims the opportunity to take proactive steps to defend themselves and mitigate the near- and long-term consequences of the Data Breach.

D. Data Breaches Pose Significant Threats

34. Data breaches have become a constant threat that, without adequate safeguards, can expose personal data to malicious actors. It is well known that PII, Social Security numbers in particular, is an invaluable commodity and a frequent target of hackers.

35. In 2022, the Identity Theft Resource Center's Annual End-of-Year Data Breach Report listed 1,802 total compromises involving 422,143,312 victims for 2022, which was just 50 compromises short of the current record set in 2021.[1] The HIPAA Journal's 2022 Healthcare Data Breach Report reported 707 compromises involving healthcare data, which is just 8 shy of the record of 715 set in 2021 and still double that of the number of similar such compromises in 2017 and triple the number of compromises in 2012.[2]

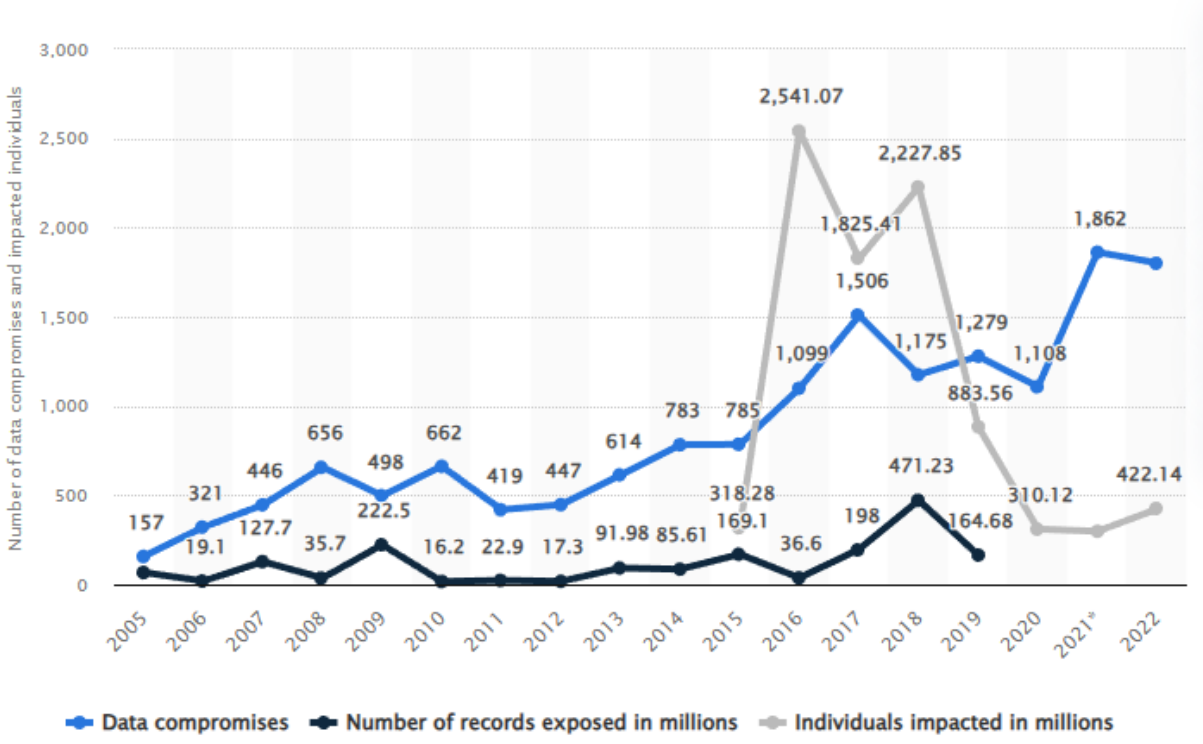
36. Statista, a German entity that collects and markets data relating to, among other things, data breach incidents and the consequences thereof, confirms that the number of data

[1] *2022 End of Year Data Breach Report*, Identity Theft Resource Center (January 25, 2023), available at:https://www.idtheftcenter.org/publication/2022-data-breach-report/?utm_source=press+release&utm_medium=web&utm_campaign=2022+Data+Breach+Report.

[2] *2022 Healthcare Data Breach Report*, The HIPAA Journal (January 24, 2023), available at: https://www.hipaajournal.com/2022-healthcare-data-breach-report/.

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

breaches has been steadily increasing since it began a survey of data compromises in 2005 with 157 compromises reported that year, to a peak of 1,862 in 2021, to 2022's total of 1,802.[3] The number of impacted individuals has also risen precipitously from approximately 318 million in 2015 to 422 million in 2022, which is an increase of nearly 50%. [4]



37. This stolen PII is then routinely traded on dark web black markets as simple commodity, with Social Security numbers being so ubiquitous to be sold at as little as $2.99 apiece and passports retailing for as little as $15 apiece.[5]

38. In addition, the severity of the consequences of a compromised Social Security number belies the ubiquity of stolen numbers on the dark web. Criminals and other unsavory

[3] *Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 2022*, Statista, available at: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.
[4] *Id.*
[5] *What is your identity worth on the dark web?* Cybernews (September 28, 2021), available at: https://cybernews.com/security/whats-your-identity-worth-on-dark-web/.

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

elements can fraudulently take out loans under the victims' name, open new lines of credit, and cause other serious financial difficulties for victims:

> [a] dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit 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. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[6]

This is exacerbated by the fact that the problems arising from a compromised Social Security number are exceedingly difficult to resolve. A victim is forbidden from proactively changing his or her number unless and until it is actually misused and harm has already occurred. And even this delayed remedial action is unlikely to undo the damage already done to the victims:

> Keep in mind that a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.[7]

39. The most sought after and expensive information on the dark web are stolen medical records which command prices from $250 to $1,000 each.[8] Medical records are considered the most valuable because unlike credit cards, which can easily be canceled, and Social Security numbers, which can be changed, medical records contain "a treasure trove of unalterable data points, such as a patient's medical and behavioral health history and

---

[6] United States Social Security Administration, *Identity Theft and Your Social Security Number*, United States Social Security Administration (July 2021), available at: https://www.ssa.gov/pubs/EN-05-10064.pdf.

[7] *Id.*

[8] Paul Nadrag, Capsule Technologies, *Industry Voices—Forget credit card numbers. Medical records are the hottest items on the dark web*, Fierce Healthcare (January 26, 2021), available at: https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web.

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

demographics, as well as their health insurance and contact information".[9] With this bounty of ill-gotten information, cybercriminals can steal victims' public and insurance benefits and bill medical charges to victims' accounts.[10] Cybercriminals can also change the victims' medical records, which can lead to misdiagnosis or mistreatment when the victims seek medical treatment.[11] Victims of medical identity theft could even face prosecution for drug offenses when cybercriminals use their stolen information to purchase prescriptions for sale in the drug trade.[12]

40. The wrongful use of compromised medical information is known as medical identity theft and the damage resulting from medical identity theft is routinely far more serious than the harm resulting from the theft of simple PII. Victims of medical identity theft spend an average of $13,500 to resolve problems arising from medical identity theft and there are currently no laws limiting a consumer's liability for fraudulent medical debt (in contrast, a consumer's liability for fraudulent credit card charges is capped at $50).[13] It is also "considerably harder" to reverse the damage from the aforementioned consequences of medical identity theft.[14]

41. Instances of Medical identity theft have grown exponentially over the years from approximately 6,800 cases in 2017 to just shy of 43,000 in 2021, which represents a seven-fold increase in the crime.[15]

42. In light of the dozens of high-profile health and medical information data breaches that have been reported in recent years, entities like Defendant charged with

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

---

[9] *Id.*
[10] *Medical Identity Theft in the New Age of Virtual Healthcare*, IDX (March 15, 2021), available at https://www.idx.us/knowledge-center/medical-identity-theft-in-the-new-age-of-virtual-healthcare. *See also* Michelle Andrews, *The Rise of Medical Identity Theft*, Consumer Reports (August 25, 2016), available at https://www.consumerreports.org/health/medical-identity-theft-a1699327549/.
[11] *Id.*
[12] *Id.*
[13] Medical Identity Theft, AARP (March 25, 2022), available at: https://www.aarp.org/money/scams-fraud/info-2019/medical-identity-theft.html.
[14] *Id.*
[15] *Id.*

maintaining and securing patient PII should know the importance of protecting that information from unauthorized disclosure. Indeed, Defendant knew, or certainly should have known, of the recent and high-profile data breaches in the health care industry: UnityPoint Health, Lifetime Healthcare, Inc., Community Health Systems, Kalispell Regional Healthcare, Anthem, Premera Blue Cross, and many others.[16]

43. In addition, the Federal Trade Commission ("FTC") has brought dozens of cases against companies that have engaged in unfair or deceptive practices involving inadequate protection of consumers' personal data, including recent cases concerning Private information against CafePress[17], LabMD, Inc., SkyMed International, Inc., and others. The FTC publicized these enforcement actions to place companies like Defendant on notice of their obligation to safeguard customer and patient information.[18]

44. Given the nature of Defendant's Data Breach, as well as the length of the time Defendant's networks were breached and the long delay in notification to the Class, it is foreseeable that the compromised Private Information has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiffs' and Class members' Private Information can easily obtain Plaintiffs' and Class members' tax returns or open fraudulent credit card accounts in Class members' names.

45. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because credit card victims can cancel or close credit and debit card accounts.[19]

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

---

[16] *See e.g.*, *Healthcare Data Breach Statistics*, HIPAA Journal, available at: https://www.hipaajournal.com/healthcare-data-breach-statistics.

[17] *In the Matter of CafePress*, C-4768 & C-4769, 1923209 (F.T.C., June 24, 2022).

[18] *See e.g.*, *In the Matter of SKYMED INTERNATIONAL, INC.*, C-4732, 1923140 (F.T.C. Jan. 26, 2021).

[19] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, Forbes (Mar 25, 2020), available at https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1. *See also Why Your Social Security Number Isn't as Valuable as Your Login Credentials*, Identity Theft Resource Center (June 18, 2021), available at https://www.idtheftcenter.org/post/why-your-social-security-number-isnt-as-valuable-as-your-login-credentials/.

The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

46. To date, Defendant has offered its consumers 2 years of identity theft monitoring services. The offered services are inadequate to protect Plaintiffs and the Class from the threats they will face for years to come, particularly in light of the Private Information at issue here.

47. Despite the prevalence of public announcements of data breach and data security compromises, its own acknowledgment of the risks posed by data breaches, and its own acknowledgment of its duties to keep Private Information private and secure, Defendant failed to take appropriate steps to protect the Private Information of Plaintiffs and the Class from misappropriation. As a result, the injuries to Plaintiffs and the Class were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for its current and former patients.

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

E. CVC Had a Duty and Obligation to Protect Private Information

48. Defendant has an obligation to protect the Private Information belonging to Plaintiffs and Class members. First, this obligation was mandated by government regulations and state laws, including HIPAA and FTC rules and regulations. Second, this obligation arose from industry standards regarding the handling of sensitive PII and medical records. And third, Defendant imposed such an obligation on itself with its promises regarding the safe handling of data. Plaintiffs and Class members provided, and Defendant obtained, their information on the understanding that it would be protected and safeguarded from unauthorized access or disclosure.

1. HIPAA Requirements and Violation

49. HIPAA requires, *inter alia*, that Covered Entities and Business Associates implement and maintain policies, procedures, systems and safeguards that ensure the confidentiality and integrity of consumer and patient PII and PHI, protect against any reasonably anticipated threats or hazards to the security or integrity of consumer and patient PII and PHI, regularly review access to data bases containing protected information, and implement

procedures and systems to detect, contain, and correct any unauthorized access to protected information. *See* 45 CFR § 164.302, *et seq.*

50. HIPAA, as applied through federal regulations, also requires private information to be stored in a manner that renders it, "unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology. . ." 45 CFR § 164.402.

51. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414 require Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***" (emphasis added).

52. Upon information and belief, Defendant failed to implement and/or maintain procedures, systems, and safeguards to protect the PII and PHI belonging to Plaintiffs and the Class from unauthorized access and disclosure.

53. Upon information and belief, Defendant's security failures include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information Defendant creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

d. 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 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents;

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

g. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii);

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

i. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3);

j. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce, in violation of 45 CFR 164.306(a)(94); and

k. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq*.

54. Upon information and belief, Defendant also failed to store the information it collected in a manner that rendered it, "unusable, unreadable, or indecipherable to unauthorized persons," in violation of 45 CFR § 164.402.

55. Defendant also violated the HIPAA Breach Notification Rule since it did not inform Plaintiffs and the Class members about the breach until 64 days after it first discovered the breach.

2. <u>FTC Act Requirements and Violations</u>

56. The FTC has promulgated numerous guides for businesses which 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. Indeed, the 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 Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

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

57. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[20] The guidelines note businesses should protect the personal 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 security problems.[21] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[22] Defendant clearly failed to do any of the foregoing, as evidenced by the length of the Data Breach, the fact that the Breach went undetected, and the amount of data exfiltrated.

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

59. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

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

---

[20] *Protecting Personal Information: A Guide for Business*, Federal Trade Comm'n (October 2016), available at https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business.

[21] *Id.*

[22] *Id.*

60. Additionally, the FTC Health Breach Notification Rule obligates companies that suffered a data breach to provide notice to every individual affected by the data breach, as well as notifying the media and the FTC. *See* 16 CFR 318.1, *et seq.*

61. As evidenced by the Data Breach, Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

62. Defendant was fully aware of its obligation to protect the Private Information of its current and former patients, including Plaintiffs and the Class, and on information and belief, Defendant is a sophisticated and technologically savvy hospital that relies extensively on technology systems and networks to maintain its practice, including storing its patients' PII, protected health information, and medical information in order to operate its business.

63. Defendant had and continues to have a duty to exercise reasonable care in collecting, storing, and protecting the Private Information from the foreseeable risk of a data breach. The duty arises out of the special relationship that exists between Defendant and Plaintiffs and Class members. Defendant alone had the exclusive ability to implement adequate security measures to its cyber security network to secure and protect Plaintiffs' and Class members' Private Information.

3. Industry Standards and Noncompliance

64. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information that they collect and maintain.

65. Some industry best practices that should be implemented by businesses dealing with sensitive PHI like Defendant include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which

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

employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

66. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

67. Defendant should have also followed the minimum standards of any one of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

68. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

4. Defendant's Own Stated Policies and Promises

69. Defendant's own published privacy policy states that CVC is committed to protecting Private Information in its possession and it admits that CVC has an obligation to make sure the Private Information it maintains is kept private.[23]

70. Clearly, Defendant failed to live up to its own stated policies and promises with regards to data privacy and data security as cybercriminals were able to infiltrate its systems and steal the Private Information belonging to Plaintiffs and Class members.

[23] *Notice of Privacy Practices*, Cardiovascular Consultants (last upd. Aptil 26, 2022), available at https://cvcheart.com/notice-of-privacy-practices/.

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

F. Plaintiffs and the Class Suffered Harm Resulting from the Data Breach

71. Like any data hack, the Data Breach presents major problems for all affected.[24]

72. The FTC warns the public to pay particular attention to how they keep personally identifying information including Social Security numbers and other sensitive data. As the FTC notes, "once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[25]

73. The ramifications of Defendant's failure to properly secure Plaintiffs' and Class members' Private Information are severe. Identity theft occurs when someone uses another person's financial, and personal information, such as that person's name, address, Social Security number, and other information, without permission in order to commit fraud or other crimes.

74. According to data security experts, one out of every four data breach notification recipients become a victim of identity fraud.

75. Furthermore, PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for an information breach to be detected.

76. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiffs and the Class at an imminent, immediate, and continuing increased risk of identity theft and identity fraud. According to a recent study published in the scholarly journal "Preventive Medicine Reports", public and corporate data breaches correlate

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

[24] Paige Schaffer, *Data Breaches' Impact on Consumers*, Insurance Thought Leadership (July 29, 2021), available at https://www.insurancethoughtleadership.com/cyber/data-breaches-impact-consumers.

[25] *Warning Signs of Identity Theft*, Federal Trade Comm'n, available at https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft.

to an increased risk of identity theft for victimized consumers.[26] The same study also found that identity theft is a deeply traumatic event for the victims, with more than a quarter of victims still experiencing sleep problems, anxiety, and irritation even six months after the crime.[27]

77. There is also a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that has not yet been exploited by cybercriminals presents a concrete risk that the cybercriminals who now possess Class members' Private Information will do so at a later date or re-sell it.

78. Data breaches have also proven to be costly for affected organizations as well, with the average cost to resolve being $4.45 million dollars in 2023.[28] The average cost to resolve a data breach involving health information, however, is more than double this figure at $10.92 million.[29]

79. The theft of medical information, beyond the theft of more traditional forms off PII, is especially harmful for victims. Medical identity theft, the misuse of stolen medical records and information, has seen a seven-fold increase over the last five years and this explosive growth far outstrips the increase in incidence of traditional identity theft.[30] Medical Identity Theft is especially nasty for victims because of the lack of laws that limit a victim's liabilities and damages from this type of identity theft (e.g., a victim's liability for fraudulent credit card charges is capped at $50), the unalterable nature of medical information, the sheer costs involved in resolving the fallout from a medical identity theft (victims spend, on average,

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

[26] David Burnes, Marguerite DeLiema, Lynn Langton, *Risk and protective factors of identity theft victimization in the United States*, Preventive Medicine Reports, Volume 17 (January 23, 2020), available at https://www.sciencedirect.com/science/article/pii/S2211335520300188?via%3Dihub.
[27] *Id.*
[28] *Cost of a Data Breach Report 2023*, IBM Security, available at https://www.ibm.com/reports/data-breach?utm_content=SRCWW&p1=Search&p4=43700072379268622&p5=p&gclid=CjwKCAjwxOymBhAFEiwAnodBLGiGtWfjX0vRlNbx6p9BpWaOo9eZY1i6AMAc6t9S8IKsxdnbBVeUbxoCtk8QAvD_BwE&gclsrc=aw.ds.
[29] *Id.*
[30] Medical Identity Theft, AARP (March 25, 2022), available at: https://www.aarp.org/money/scams-fraud/info-2019/medical-identity-theft.html.

$13,500 to resolve problems arising from this crime), and the risk of criminal prosecution under anti-drug laws.[31]

80. In response to the Data Breach, Defendant offered to provide certain individuals whose Private Information was exposed in the Data Breach with 2-years of identity theft protection and credit monitoring. However, 2 years is much shorter than what is necessary to protect against the lifelong risk of harm imposed on Plaintiffs and Class members by Defendant's failures.

81. Moreover, the credit monitoring offered by Defendant is fundamentally inadequate to protect them from the injuries resulting from the unauthorized access and exfiltration of their sensitive Private Information.

82. Here, due to the Breach, Plaintiffs and Class members have been exposed to injuries that include, but are not limited to:

a. Theft of Private Information;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of financial accounts as a direct and proximate result of the Private Information stolen during the Data Breach;

c. Damages arising from the inability to use accounts that may have been compromised during the Data Breach;

d. Costs associated with spending time to address and mitigate the actual and future consequences of the Data Breach, such as finding fraudulent charges, cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, placing freezes and alerts on their credit reports, contacting their financial institutions to notify them that their personal information was exposed and to dispute fraudulent charges, imposition of withdrawal and purchase limits on compromised accounts, including but not limited to lost productivity and opportunities, time taken from the enjoyment of one's life, and the inconvenience, nuisance, and annoyance of dealing with all issues resulting from the Data Breach, if they were fortunate enough to learn of the Data Breach despite Defendant's delay in disseminating notice in accordance with state law;

[31] *Id.*

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

e. The imminent and impending injury resulting from potential fraud and identity theft posed because their Private Information is exposed for theft and sale on the dark web; and

f. The loss of Plaintiffs' and Class members' privacy.

83. Plaintiffs and Class members have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their Private Information being accessed by cybercriminals, risks that will not abate within a mere 2 years.

84. As a direct and proximate result of Defendant's acts and omissions in failing to protect and secure Private Information, Plaintiffs and Class members have been placed at a substantial risk of harm in the form of identity theft, and have incurred and will incur actual damages in an attempt to prevent identity theft.

85. Plaintiffs retain an interest in ensuring there are no future breaches, in addition to seeking a remedy for the harms suffered as a result of the Data Breach on behalf of both themselves and similarly situated individuals whose Private Information was accessed in the Data Breach.

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

G. EXPERIENCES SPECIFIC TO PLAINTIFFS

1. Plaintiff Michele Stroup's Experience

86. Plaintiff Stroup was a patient of CVC.

87. Plaintiff Stroup received CVC's data breach notice. The notice informed Plaintiff Stroup that her Private Information had been improperly accessed and obtained by third parties.

88. As a result of the Data Breach, Plaintiff Stroup has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. She has also spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities, including, but not limited to, work and recreation.

89. As a result of the Data Breach, Plaintiff Stroup has suffered anxiety due to the public dissemination of her personal information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and using her private information for purposes of identity theft and fraud. Plaintiff Stroup is concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

90. Plaintiff Stroup suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Defendant obtained from her; (b) violation of her privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

91. As a result of the Data Breach, Plaintiff Stroup anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. And, as a result of the Data Breach, she is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

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

2. Plaintiff Georgios Asimakopoulos's Experience

92. Plaintiff Asimakopoulos was a patient of CVC.

93. Plaintiff Asimakopoulos received CVC's data breach notice. The notice informed him that his Personal Information had been improperly accessed and obtained by third parties.

94. After the breach, Plaintiff Asimakopoulos was informed, by Equifax, that somebody had attempted to take out a loan for $11,000 in his name.

95. As a result of the Data Breach, and this attempted fraud, Plaintiff Asimakopoulos has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. He has also spent several hours dealing with the Data Breach, valuable time he otherwise would have spent on other activities, including, but not limited to, work and recreation.

96. As a result of the Data Breach, Plaintiff Asimakopoulos has suffered anxiety due to the public dissemination of his personal information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and using his information for purposes of identity theft and fraud. Plaintiff Asimakopoulos is concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

97. Plaintiff Asimakopoulos suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from her; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

98. As a result of the Data Breach, Plaintiff Asimakopoulos anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. And, as a result of the Data Breach, he is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

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

V. CLASS REPRESENTATION ALLEGATIONS

99. Plaintiffs bring this action on behalf of themselves and a putative class pursuant to Ariz. R. Civ. P. 23 defined as follows:

> All persons in the United States whose Private Information was accessed in the Data Breach.

Excluded from the Class are Defendant, its executives and officers, and the Judge(s) assigned to this case. Plaintiffs reserve the right to modify, change or expand the Class definition after conducting discovery.

100. Numerosity: Upon information and belief, the Class is so numerous that joinder of all members is impracticable with the number of affected individuals estimated to be in the tens of thousands. The exact number and identities of individual members of the Class are

unknown at this time, such information being in the sole possession of Defendant and obtainable by Plaintiffs only through the discovery process. The members of the Class will be identifiable through information and records in Defendant's possession, custody, and control.

101. Existence and Predominance of Common Questions of Fact and Law: Common questions of law and fact exist as to all members of the Class. These questions predominate over the questions affecting individual Class members. These common legal and factual questions include, but are not limited to:

a. When Defendant learned of the Data Breach;

b. Whether hackers obtained Class Members' Private Information via the Data Breach;

c. Whether Defendant's response to the Data Breach was adequate;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

e. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations, industry standards, and/or its own promises and representations;

f. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

g. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

h. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

i. Whether Defendant had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and the Class Members;

j. Whether Defendant breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

k. Whether Defendant's conduct violated the FTCA, HIPAA, and/or the Consumer Protection Act invoked herein;

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

l. Whether Defendant's conduct was negligent;

m. Whether Defendant's conduct was *per se* negligent;

n. Whether Defendant was unjustly enriched;

o. What damages Plaintiffs and Class Members suffered as a result of Defendant's misconduct;

p. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages;

q. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

r. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

102. Typicality: All of Plaintiffs' claims are typical of the claims of the Class since Plaintiffs and all members of the Class had their Private Information compromised in the Data Breach. Plaintiffs' claims and damages are also typical of the Class because they resulted from Defendant's uniform wrongful conduct. Likewise, the relief to which Plaintiffs are entitled to is typical of the Class because Defendant has acted, and refused to act, on grounds generally applicable to the Class.

103. Adequacy: Plaintiffs are adequate class representatives because their interests do not materially or irreconcilably conflict with the interests of the Class they seek to represent, they have retained counsel competent and highly experienced in complex class action litigation, and intend to prosecute this action vigorously. Plaintiffs and their counsel will fairly and adequately protect the interests of the Class. Neither Plaintiffs nor their counsel have any interests that are antagonistic to the interests of other members of the Class.

104. Superiority: Compared to all other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class, a class action is the most superior. The

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

injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Defendant's conduct. It would be virtually impossible for members of the Class individually to effectively redress the wrongs done to them. Even if the members of the Class could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties and to the court system presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Members of the Class can be readily identified and notified based on, *inter alia*, Defendant's records and databases.

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

VI. CAUSES OF ACTION

COUNT I
NEGLIGENCE
(By Plaintiffs on behalf of the Class)

105. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

106. Defendant owes a duty of care to protect the Private Information belonging to Plaintiffs and Class Members. Defendant also owes several specific duties including, but not limited to, the duty:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. to protect patients' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. to have procedures in place to detect the loss or unauthorized dissemination of Private Information in its possession;

d. to employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class Members pursuant to the FTCA;

e. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. to promptly notify Plaintiffs and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

107. Defendant also owes this duty because Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 requires Defendant to use reasonable measures to protect confidential data.

108. Defendant also owes this duty because industry standards mandate that Defendant protect its patients' confidential private information.

109. Defendant also owes this duty because it had a special relationship with Plaintiffs' and Class members. Plaintiffs and Class members entrusted their Private Information to Defendant on the understanding that adequate security precautions would be taken to protect this information. Furthermore, only Defendant had the ability to protect its systems and the Private Information stored on them from attack.

110. Defendant also owes a duty to timely disclose any unauthorized access and/or theft of the Private Information belonging to Plaintiffs and the Class. This duty exists to allow Plaintiffs and the Class the opportunity to undertake appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their Private Information.

111. Defendant breached its duties to Plaintiffs and the Class by failing to take reasonable appropriate measures to secure, protect, and/or otherwise safeguard the Private Information belonging to Plaintiffs and Class members.

112. Defendant also breached the duties it owed to Plaintiffs and the Class by failing to timely and accurately disclose to Plaintiffs and Class members that their Private Information had been improperly acquired and/or accessed.

113. As a direct and proximate result of Defendant's conduct, Plaintiffs and the Class were damaged. These damages include, and are not limited to:

- Lost or diminished value of their Private Information;

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

- Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information;

- Lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges;

- Permanent increased risk of identity theft.

114. Plaintiffs and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant and the damages they suffered were the foreseeable result of the aforementioned inadequate security practices.

115. In failing to provide prompt and adequate individual notice of the Data Breach, Defendant also acted with reckless disregard for the rights of Plaintiffs and Class Members.

116. Plaintiffs are entitled to damages in an amount to be proven at trial and injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT II
NEGLIGENCE *PER SE*
(By Plaintiffs on behalf of the Class)

117. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

118. Section 5 of the FTCA imposes a duty on Defendant to provide fair and adequate data security to secure, protect, and/or otherwise safeguard the Private Information of Plaintiffs and Class Members.

119. HIPAA imposes a duty on Defendant to implement reasonable safeguards to protect Plaintiffs' and Class Members' Private Information. 42 U.S.C. § 1302(d), *et seq*.

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

120. HIPAA also requires Defendant to render unusable, unreadable, or indecipherable all Private Information it collected. Defendant was required to do so through "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key." *See* definition of "encryption" at 45 C.F.R. § 164.304.

121. In the event of a data breach, HIPAA obligates Covered Entities and Business Associates to notify affected individuals, prominent media outlets, and the Secretary of the Department of Health and Human Services of the data breach without unreasonable delay and in no event later than 60 days after discovery of the data breach. 45 CFR § 164.400, *et seq.*

122. Defendant violated the FTCA and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to secure, protect, and/or otherwise safeguard Plaintiffs' and Class Members' Private Information.

123. Defendant violated HIPAA by failing to properly encrypt the Private Information it collected.

124. Defendant violated HIPAA by unduly delaying reasonable notice of the actual breach until 64 days after it discovered the intrusion and *at least* 66 days after the breach first occurred.

125. Defendant's failure to comply with HIPAA and the FTCA constitutes negligence *per se*.

126. Plaintiffs and Class Members are within the class of persons that the FTCA and HIPAA are intended to protect.

127. It was reasonably foreseeable that the failure to protect and secure Plaintiffs' and Class Members' Private Information in compliance with applicable laws and industry standards would result in that Information being accessed and stolen by unauthorized actors.

128. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to theft of their

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

personal information, damages from the lost time and effort to mitigate the impact of the Data Breach, and permanently increased risk of identity theft.

129. Plaintiffs and Class Members are entitled to damages in an amount to be proven at trial and injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT III
BREACH OF IMPLIED CONTRACT
(By Plaintiffs on behalf of the Class)

130. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

131. Plaintiffs and the Class provided Defendant with their Private Information.

132. By providing their Private Information, and upon Defendant's acceptance of this information, Plaintiffs and the Class, on one hand, and Defendant, on the other hand, entered into implied-in-fact contracts for the provision of data security, separate and apart from any express contract entered into between the parties.

133. The implied contracts between Defendant and Plaintiffs and Class members obligated Defendant to take reasonable steps to secure, protect, safeguard, and keep confidential Plaintiffs' and Class members' Private Information. The terms of these implied contracts are described in federal laws, state laws, and industry standards, as alleged above. Defendant expressly adopted and assented to these terms in its public statements, representations and promises as described above.

134. The implied contracts for data security also obligated Defendant to provide Plaintiffs and Class members with prompt, timely, and sufficient notice of any and all unauthorized access or theft of their Private Information.

135. Defendant breached these implied contracts by failing to take, develop and implement adequate policies and procedures to safeguard, protect, and secure the Private Information belonging to Plaintiffs and Class members; allowing unauthorized persons to

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

access Plaintiffs' and Class members' Private Information; and failing to provide prompt, timely, and sufficient notice of the Data Breach to Plaintiffs and Class members, as alleged above.

136. As a direct and proximate result of Defendant's breaches of the implied contracts, Plaintiffs and the Class have been damaged as described herein, will continue to suffer injuries as detailed above due to the continued risk of exposure of Private Information, and are entitled to damages in an amount to be proven at trial.

COUNT IV
UNJUST ENRICHMENT
(By Plaintiffs on behalf of the Class)

137. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

138. This count is brought in the alternative to Count III.

139. Plaintiffs and the Class have a legal and equitable interest in their Private Information that was collected and maintained by Defendant.

140. Defendant was benefitted by the conferral upon it of Plaintiffs' and Class members' Private Information and by its ability to retain and use that information. Defendant understood that it was in fact so benefitted.

141. Defendant also understood and appreciated that Plaintiffs' and Class members' Private Information was private and confidential and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

142. But for Defendant's willingness and commitment to maintain its privacy and confidentiality, Plaintiffs and Class members would not have provided or authorized their Private Information to be provided to Defendant, and Defendant would have been deprived of the competitive and economic advantages it enjoyed by falsely claiming that its data-security safeguards met reasonable standards. These competitive and economic advantages include, without limitation, wrongfully gaining patients, gaining the reputational advantages conferred upon it by Plaintiffs and Class members, collecting excessive advertising and sales revenues as

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

described herein, monetary savings resulting from failure to reasonably upgrade and maintain data technology infrastructures, staffing, and expertise raising investment capital as described herein, and realizing excessive profits.

143. As a result of Defendant's wrongful conduct as alleged herein (including, among other things, its deception of Plaintiffs, the Class, and the public relating to the nature and scope of the data breach; its failure to employ adequate data security measures; its continued maintenance and use of the Private Information belonging to Plaintiffs and Class members without having adequate data security measures; and its other conduct facilitating the theft of that Private Information), Defendant has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and the Class.

144. Defendant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiffs' and Class members' sensitive Private Information, while at the same time failing to maintain that information secure from intrusion.

145. Under the common law doctrine of unjust enrichment, it is inequitable for Defendant to be permitted to retain the benefits it received, and is still receiving, without justification, from Plaintiffs and the Class in an unfair and unconscionable manner. Defendant's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

146. The benefit conferred upon, received, and enjoyed by Defendant was not conferred officiously or gratuitously, and it would be inequitable and unjust for Defendant to retain the benefit.

147. Defendant is therefore liable to Plaintiffs and the Class for restitution in the amount of the benefit conferred on Defendant as a result of its wrongful conduct, including specifically the value to Defendant of the PII and medical information that was accessed and exfiltrated in the Data Breach and the profits Defendant receives from the use and sale of that information.

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

148. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct.

149. Plaintiffs and Class Members may not have an adequate remedy at law against Defendant, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT V
VIOLATION OF THE ARIZONA CONSUMER FRAUD ACT
A.R.S. s 44-1521, *et seq.*
(By Plaintiffs on behalf of the Class)

150. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

151. Plaintiffs and Class members are "consumers" under the Arizona Consumer Fraud Act ("ACFA").

152. Defendant is engaged in, and its acts and omissions affect, trade and commerce. Defendant's relevant acts, practices and omissions complained of in this action were done in the course of Defendant's business of marketing, offering for sale, and selling goods and services throughout Arizona.

153. The ACFA makes it illegal for a business to engage in or use, "any deception, deceptive or unfair act or practice, fraud, false pretense, false promise, misrepresentation, or concealment, suppression or omission," in connection with any sale or advertisement. A.R.S. § 44-1522.

154. Defendant's deceptive or unfair acts or practices in the conduct of business include, but are not limited to:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and

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

privacy measures following previous cybersecurity incidents in the industry, which were direct and proximate causes of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' Private Information, including but not limited to duties imposed by the FTC Act, which were direct and proximate causes of the Data Breach;

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

e. Misrepresenting that it would comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiffs' and Class members' Private Information;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class members' Private Information;

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiffs' and Class members' Private Information; and

h. Failing to promptly and adequately notify Plaintiffs and the Class that their Private Information was accessed by unauthorized persons in the Data Breach.

155. Defendant's practices were also contrary to legislatively declared and public policies that seek to protect data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected in laws, such as HIPAA and the FTC Act.

156. The injuries suffered by Plaintiffs and the Class greatly outweigh any potential countervailing benefit to consumers or to competition, and are not injuries that Plaintiffs and the Class should or could have reasonably avoided.

157. The damages, ascertainable losses and injuries, including to their money or property, suffered by Plaintiffs and the Class as a direct result of Defendant's deceptive acts

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

and practices as set forth herein include, without limitation:

a. unauthorized charges on their debit and credit card accounts;

b. theft of their Private Information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse effects on their credit scores and adverse credit notations;

e. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate and mitigate the actual and future consequences of the Data Breach, including without limitation finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

f. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

g. damages to and diminution in value of their personal information entrusted to Defendant, and with the understanding that it would safeguard their data against theft and not allow access and misuse of their data by others; and

h. the continued risk to their Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as it fails to undertake appropriate and adequate measures to protect data in its possession.

158. Plaintiffs and the Class seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; declaratory and injunctive relief, including an injunction barring Defendant from disclosing their Private Information without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper under the Arizona Consumer Fraud Act.

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

COUNT VI
INTRUSION UPON SECLUSION
(By Plaintiffs on behalf of the Class)

159. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

160. Plaintiffs and Class members had a reasonable expectation of privacy in the Private Information that Defendant possessed and/or continues to possess.

161. By failing to keep Plaintiffs' and Class members' Private Information safe, and by misusing and/or disclosing their Private Information to unauthorized parties for unauthorized use, Defendant invaded Plaintiffs' and Class members' privacy by:

a. Intruding into their private affairs in a manner that would be highly offensive to a reasonable person; and

b. Publicizing private facts about Plaintiffs and Class members, which is highly offensive to a reasonable person.

162. Defendant knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiffs' position would consider Defendant's actions highly offensive.

163. Defendant invaded Plaintiffs' and Class members' right to privacy and intruded into Plaintiffs' and Class members' private affairs by misusing and/or disclosing their private information without their informed, voluntary, affirmative, and clear consent.

164. As a proximate result of such misuse and disclosures, Plaintiffs' and Class members' reasonable expectation of privacy in their Private Information was unduly frustrated and thwarted. Defendant's conduct amounted to a serious invasion of Plaintiffs' and Class members' protected privacy interests.

165. In failing to protect Plaintiffs' and Class members' Private Information, and in misusing and/or disclosing their Private Information, Defendant has acted with malice and oppression and in conscious disregard of Plaintiffs' and the Class members rights to have such information kept confidential and private, in failing to provide adequate notice, and in placing its own economic, corporate, and legal interests above the privacy interests of its millions of patients. Plaintiffs, therefore, seek an award of damages, including punitive damages, on behalf

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

of Plaintiffs and the Class.

PRAYER FOR RELIEF

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

A. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiffs are proper class representatives; and appoint Plaintiffs' Counsel as Class Counsel;

B. That the Court grant permanent injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein;

C. That the Court award Plaintiffs and the Class members compensatory, consequential, and general damages in an amount to be determined at trial;

D. That the Court award Plaintiffs and the Class members statutory damages, and punitive or exemplary damages, to the extent permitted by law;

E. That the Court award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

F. That the Court award pre- and post-judgment interest at the maximum legal rate;

G. That the Court award grant all such equitable relief as it deems proper and just, including, but not limited to, disgorgement and restitution; and

H. That the Court grant all other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

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

. . . .

. . . .

. . . .

. . . .

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

RESPECTFULLY SUBMITTED this 21st day of December, 2023.

PEREZ LAW GROUP, PLLC

/s/ Cristina Perez Hesano
Cristina Perez Hesano, Esq.
Attorneys for Plaintiffs

Daniel O. Herrera
Nickolas J. Hagman
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
Attorneys for Plaintiffs and the Proposed Class

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