Exhibit A1

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 **FIRST AMENDED CLASS ACTION COMPLAINT** **CLASS REPRESENTATION** (Jury Trial Requested) (Assigned to the Honorable Katherine Cooper)

Plaintiffs Michele Stroup, Georgios Asimakopoulos, Brian Hazlett, Dode Hammack, Peter Fiorentino, and John Gatchell ("Plaintiffs"), individually, and on behalf of all others similarly situated, bring this action against Defendant 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 medical consultations, advanced testing, and outpatient rehabilitation services. CVC is the largest provider of cardiovascular medicine in Arizona.[1]

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. 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 their financial guarantors, including Plaintiffs and nearly 500,000[2] Class members (the "Breach" or the "Data Breach").

4. By the time Defendant discovered the Breach on September 29, 2023, it was too late. Before CVC was able to secure its systems, hackers accessed and stole its patients' highly sensitive Private Information, including: names, mailing addresses, dates of birth, demographic and contact information, emergency contact information, Social Security numbers, driver's license and state ID numbers, insurance policy and guarantor information, diagnosis and treatment information, and other information contained in patients' medical and billing records.

[1] CVC, *About Cardiovascular Consultants*, https://cvcheart.com/about/ (last visited March 5, 2024).
[2] *See* U.S. Department of Health and Human Services, *Cases Currently Under Investigation*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Mar. 5, 2024).

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

Hackers also compromised Private Information pertaining to patients' financial guarantors, including: names, dates of birth, email addresses, telephone numbers, and mailing addresses, and in the case of primary policy holders/insurance subscribers, Social Security numbers and insurance information.[3]

5. On December 2, 2023, Defendant mailed notice letters to individuals whose information was accessed and stolen in the Data Breach.[4]

6. Plaintiffs and the Class entrusted their Private Information to Defendant in order to receive medical care and services, and they reasonably expected Defendant to safeguard their information. Accordingly, Defendant had a duty and obligation to protect Plaintiffs' and Class members' Private Information and prevent unauthorized third parties from accessing it.

7. Defendant failed to fulfill this obligation, as evidenced by the cybercriminals' successful breach of CVC's information systems and databases, resulting in the unauthorized access and theft of vast quantities of Private Information belonging to Defendant's patients and their 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.

8. The Data Breach occurred because Defendant failed to implement reasonable security protections to safeguard its information systems and databases. Defendant also failed to inform its patients, who entrusted Defendant with their Private Information, that its data security practices were deficient and inadequate.

9. Defendant's subsequent handling of the Data Breach was also deficient: Defendant failed to timely detect the Data Breach and unreasonably delayed in notifying victims for more than 64 days after the Breach was discovered.

10. As a result of Defendant's negligent, reckless, intentional, and/or unconscionable failure to adequately satisfy its contractual, statutory, and common-law obligations, Plaintiffs

[3] *See Notice of Data Breach*, CVC (Dec. 4, 2023), https://cvcheart.com/notice/.
[4] *See id.*

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

and Class members suffered injuries, 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;
- 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;
- Loss of time needed to change usernames and passwords on their accounts;
- Loss of time needed to investigate, correct and resolve unauthorized access to their accounts;
- Loss of 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.

11. Accordingly, Plaintiffs bring this action, individually and 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 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

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

PARTIES

Plaintiff Michele Stroup

12. 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

13. 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.

Plaintiff Brian Hazlett

14. Plaintiff Brian Hazlett is a resident and citizen of Glendale, Arizona. Plaintiff Hazlett was a patient of CVC. Plaintiff Hazlett received Defendant's Data Breach Notice.

Plaintiff Dode Hammack

15. Plaintiff Dode Hammack is a resident and citizen of Wyoming. Plaintiff Hammack was a patient of CVC. Plaintiff Hazlett received Defendant's Data Breach Notice.

Plaintiff Peter Fiorentino

16. Plaintiff Peter Fiorentino is a resident and citizen of Phoenix, Arizona. Plaintiff Fiorentino was a patient of CVC. Plaintiff Hazlett received Defendant's Data Breach Notice.

Plaintiff John Gatchell

17. Plaintiff John Gatchell is a resident and citizen of Anthem, Arizona. Plaintiff Gatchell is a current patient of CVC. Plaintiff Gatchell received Defendant's Data Breach Notice.

Defendant Cardiovascular Consultants, Ltd.

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

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

JURISDICTION AND VENUE

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

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

21. 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

22. Defendant CVC holds itself out as "the largest provider of cardiovascular medicine in Arizona and the Southwestern U.S."[5] In the course of its operations as a medical provider, and in order to facilitate the for-profit delivery of medical treatment, CVC collects troves of Private Information from its patients, and/or their financial guarantors, including, but not limited to:

- Patients: names, mailing addresses, dates of birth, demographic and contact information, emergency contact information, Social Security numbers, driver's license and state ID numbers, insurance policy and guarantor information, diagnosis and treatment information, and other information from medical and billing records.

- Financial Guarantors: names, dates of birth, email addresses, telephone numbers, and mailing addresses.

- Primary Policyholders and Subscribers: names, mailing addresses, telephone numbers, dates of birth, Social Security numbers, and insurance information.

23. CVC failed to implement necessary data security safeguards, as evidenced by cybercriminals' successful exfiltration of copious amounts of Private Information belonging to

[5] CVC, *About Us*, https://cvcheart.com/about/ (last visited Mar. 5, 2024).

CVC's current and former patients and patients' guarantors—including Plaintiffs and Class members.

24. 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 their information would keep that sensitive and 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.

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

26. 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.

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

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

27. On or before September 27, 2023, cybercriminals breached and accessed CVC's systems.[6]

28. On September 29, 2023, CVC discovered the intrusion and began an investigation.[7]

29. While the complete scope of the Breach is not yet clear, cybercriminals appear to have accessed and exfiltrated most of the Private Information collected, stored, and maintained by CVC. Indeed, a forensic investigation commissioned by Defendant determined that unknown cybercriminals accessed, obtained, and exfiltrated the Private Information of approximately 500,000 affected individuals.[8]

---

[6] *Notice of Data Breach*, CVC (Dec. 4, 2023), https://cvcheart.com/notice/.

[7] *Id.*

[8] *Fresenius Medical Care AG Form 6-K*, SEC (Dec. 6, 2023), available at https://www.sec.gov/Archives/edgar/data/1333141/000110465923123839/tm2332190d2_6k.htm.

30. Upon information and belief, the "Qilin" ransomware group was responsible for perpetrating the Data Breach. On October 25, 2023, members of this group claimed credit for the attack through a post made on its dark web data leak website.[9]

31. The same post also included a download link to a 205.93 GB compressed archive, which Qilin advertised as containing "all personal data of clients and employees of [CVC]":[10]

32. On December 2, 2023, CVC mailed data breach notice letters to the nearly half a million individuals whose Private Information was compromised in the Data Breach.[11]

33. For its part, CVC has acknowledged the severity of the Data Breach. In the notice letter issued to victims, CVC: confirmed that "the attacker(s) accessed certain systems, encrypted information, and stole some [CVC] information, which included personal information of [CVC's] patients"; admitted that it had to "implement[ ] additional safeguards, to help prevent similar incidents in the future"; and encouraged victims to "remain alert by regularly reviewing [their] account statements and monitoring free credit reports, and immediately report to [their] banks and other financial institutions any suspicious activity involving [their] accounts."

---

[9] *Cardiovascular Consultants (CVC Heart) Allegedly hit by Ransomware*, Databreaches.net (Nov. 6, 2023), https://www.databreaches.net/cardiovascular-consultants-cvc-heart-allegedly-hit-by-ransomware/.

[10] *Id.*

[11] *See Notice of Data Breach*, CVC (Dec. 4, 2023), https://cvcheart.com/notice/.

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

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

34. 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 result of multiple failings on the part of Defendant.

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

36. 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.

37. In addition to the failures that led to the Data Breach, Defendant's failings in handling and responding to the Data Breach exacerbated the resulting harm to Plaintiffs and the Class.

38. Defendant failed to timely inform Plaintiffs and Class members that their information was stolen, waiting 64 days after it detected the Data Breach to finally provide notice to affected individuals. This delay virtually ensured that the cybercriminals who stole the 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.

39. Additionally, Defendant's attempt to ameliorate the effects of the Data Breach with abbreviated, non-automatic 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 theft and misuse of their Private Information. And this can, and in some circumstances already has, caused irreparable harm to their personal, financial, reputational,

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

and future well-being. This harm is even more acute because much of the stolen Private Information, such as healthcare data, is immutable.

40. In short, Defendant's myriad failures, including the failure to timely detect the 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 protect themselves and mitigate the near- and long-term consequences of the Data Breach.

D. Data Breaches Pose Significant Threats

41. 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.

42. In 2023, the Identity Theft Resource Center's Annual End-of-Year Data Breach Report listed 3,205 total compromises involving 353,027,892 victims for 2023, representing "an all-time high for data compromises reported in the United States."[12]

43. According to the HIPAA Journal's 2023 Healthcare Data Breach Report, "[a]n unwanted record was set in 2023 with 725 large security breaches in healthcare reported to the Department of Health and Human Services Office for Civil Rights, beating the record of 720 healthcare security breaches set the previous year."[13]

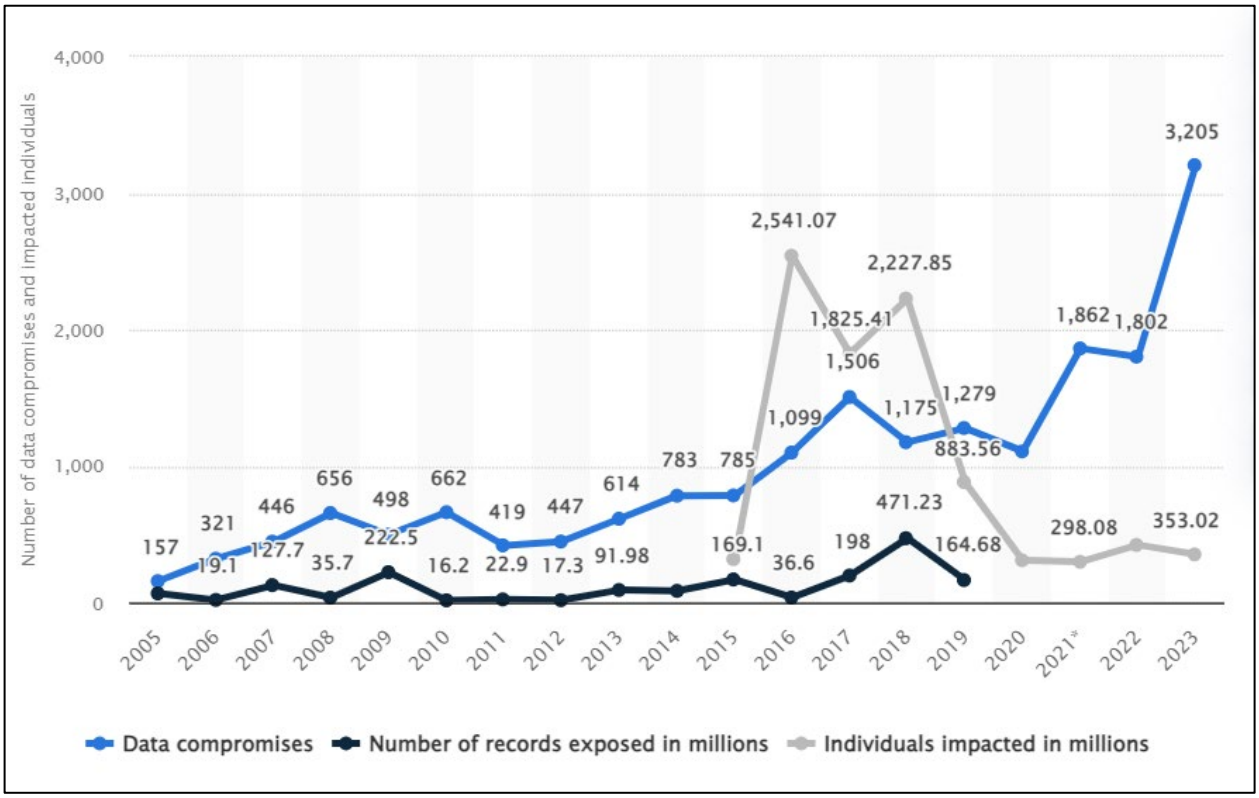
44. Statista, a German entity that collects and markets data relating to data breach incidents and their consequences, confirms that the number of data breaches has been steadily increasing since it began a survey of data compromises in 2005; it reported 157 compromises

[12] *2023 Annual Data Breach Report*, Identity Theft Resource Center (Jan. 2024), available at https://www.idtheftcenter.org/publication/2023-data-breach-report/.

[13] Steve Adler, *Security Breaches in Healthcare in 2023*, The HIPAA Journal (Jan. 31, 2024), available at https://www.hipaajournal.com/wp-content/uploads/2024/01/Security_Breaches_In_Healthcare_in_2023_by_The_HIPAA_Journal.pdf.

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

in 2005, 1,802 in 2022, and a peak of 3,205 in 2023.[14] 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%.[15]



45. Stolen PII is routinely traded on dark web black markets as a 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.[16]

46. In addition, the severity of the consequences of a compromised Social Security number belies the ubiquity of stolen numbers on the dark web. Armed with just a name and

[14] *Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 2023*, Statista (Feb. 12, 2024), https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.

[15] *Id.*

[16] Edvardas Mikalauskas, *What is your identity worth on the dark web?*, Cybernews (September 28, 2021), https://cybernews.com/security/whats-your-identity-worth-on-dark-web/.

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

Social Security number, criminals and other unsavory 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.[17]

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.[18]

47. The most sought after and expensive information on the dark web are stolen medical records which command prices from $250 to $1,000 each.[19] Medical records are

[17] 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.

[18] *Id.*

[19] 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), 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

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 demographics, as well as their health insurance and contact information."[20] With this bounty of ill-gotten information, cybercriminals can steal victims' public and insurance benefits and bill medical charges to victims' accounts.[21] Cybercriminals can also change the victims' medical records, which can lead to misdiagnosis or mistreatment when the victims seek medical treatment.[22] 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.[23]

48. 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).[24] It is also "considerably harder" to reverse the damage from the aforementioned consequences of medical identity theft.[25]

49. 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

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

---

[20] *Id.*
[21] *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), https://www.consumerreports.org/health/medical-identity-theft-a1699327549/.
[22] *Id.*
[23] *Id.*
[24] *Medical Identity Theft*, AARP (March 25, 2022), https://www.aarp.org/money/scams-fraud/info-2019/medical-identity-theft.html.
[25] *Id.*

increase in the crime.[26]

50. In light of the dozens of high-profile health and medical information data breaches that have been reported in recent years, entities that are charged with maintaining and securing patient PII and PHI, like Defendant, 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.[27]

51. 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,[28] 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.[29]

52. 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.

53. 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

---

[26] *Id.*

[27] *See e.g.*, *Healthcare Data Breach Statistics*, The HIPAA Journal, available at: https://www.hipaajournal.com/healthcare-data-breach-statistics (last visited Mar. 5, 2024).

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

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

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

data breach, because credit card victims can cancel or close credit and debit card accounts.[30] The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

54. To date, Defendant has offered victims of the Data Breach 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.

55. 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

56. 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

[30] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, Forbes (Mar 25, 2020), 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), https://www.idtheftcenter.org/post/why-your-social-security-number-isnt-as-valuable-as-your-login-credentials/.

the understanding that it would be protected and safeguarded from unauthorized access or disclosure.

1. HIPAA Requirements and Violations

57. 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 databases 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.*

58. 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.

59. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires 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***." *Id.* (emphasis added).

60. 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.

61. 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);

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

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;

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.*

62. 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.

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

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

64. The FTC has promulgated numerous guides for businesses that highlight the

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

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).

65. 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.[31] 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.[32] 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.[33] 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.

66. 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.

---

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

[32] *Id.*

[33] *Id.*

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

67. 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.

68. 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.*

69. 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.

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

71. Defendant had and continues to have a duty to exercise reasonable care in collecting, storing, and protecting 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. <u>Industry Standards and Noncompliance</u>

72. As noted above, experts studying cybersecurity routinely identify healthcare entities, like Defendant, as being particularly vulnerable to cyberattacks because of the value of the Private Information they collect and maintain.

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

73. Some industry best practices that should be implemented by businesses dealing with sensitive Private Information, 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 employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

74. 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.

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

75. 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.

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

77. The FTC also recommends the following best practices to deter cyberattacks:

- 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.
- 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.

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

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[34]

4. Defendant's Own Stated Policies and Promises

78. Defendant's own published privacy policy states that CVC is committed to protecting Private Information in its possession and acknowledges CVC's obligation to make sure the Private Information it maintains is kept private.[35]

79. 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.

F. Defendant was Negligent in its handling of Private Information belonging to Plaintiffs and the Class

80. Defendant participated in and controlled the development, implementation and enforcement of its privacy policy and controlled the process of gathering Private Information from Plaintiff and Class members.

81. Defendant therefore assumed and otherwise owed duties and obligations to Plaintiff and Class members to take reasonable measures to protect their Private Information, including the duty of oversight, training, instruction, and testing of its data security policies and network systems. Defendant breached these obligations to Plaintiff and Class members and/or was otherwise negligent because it failed to properly implement data security systems and policies that would adequately safeguard Plaintiffs' and Class members' Private Information. Upon information and belief, Defendant's unlawful conduct included, but is not limited to, one or more of the following acts and/or omissions:

---

[34] *See generally Fighting Identity Theft With the Red Flags Rule: A How-To Guide for Business*, FED. TRADE COMM., https://www.ftc.gov/business-guidance/resources/fighting-identity-theft-red-flags-rule-how-guide-business (last accessed May 1, 2023).

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

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

a. Failing to design and maintain an adequate data security system to reduce the risk of data breaches and protect Plaintiffs' and Class members' Private Information;

b. Failing to properly monitor its data security systems for data security vulnerabilities and risk;

c. Failing to test and assess the adequacy of its data security system(s);

d. Failing to develop adequate training programs related to the proper handling of emails and email security practices;

e. Failing to develop and put into place uniform procedures and data security protections for its healthcare network;

f. Failing to adequately fund and allocate resources for the adequate design, operation, maintenance, and updating necessary to meet industry standards for data security protection;

g. Failing to require a data security system to ensure the confidentiality and integrity of electronic PHI its network created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

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

i. 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)(i);

j. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

k. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI, in violation of 45 C.F.R. § 164.306(a)(2);

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

m. Failing to ensure that it was compliant with HIPAA security standard rules by its workforces, in violation of 45 C.F.R. § 164.306(a)(4);

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

n. Failing to train all members of its workforce effectively on the policies and procedures regarding PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b);

o. Failing to ensure that the electronic PHI it maintained is unusable, unreadable, or indecipherable to unauthorized individuals, as Defendant had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR 164.304 definition of encryption).

p. Failing to ensure or otherwise require that it was compliant with FTC guidelines for cybersecurity;

q. Failing to ensure or otherwise require that it was adhering to one or more of the industry standards for cybersecurity discussed above;

r. Failing to implement or update antivirus and malware protection software in need of security updating;

s. Failing to require encryption or adequate encryption on its data systems; and

t. Otherwise negligently and unlawfully failing to safeguard Plaintiffs' and Class members' Private Information provided to Defendant, which in turn allowed cyberthieves to access its IT systems.

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

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

82. Like any data hack, the Data Breach presents major problems for all affected.[36]

83. The FTC warns the public to pay particular attention to how they keep personally identifiable 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

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

account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[37]

84. 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.

85. 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.

86. 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 to an increased risk of identity theft for victimized consumers.[38] 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.[39]

87. 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.

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

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

[38] David Burnes, Marguerite DeLiema, Lynn Langton, *Risk and protective factors of identity theft victimization in the United States*, Preventive Medicine Reports, Volume 17 (Jan. 23, 2020), available at https://www.sciencedirect.com/science/article/pii/S2211335520300188?via%3Dihub.

[39] *Id.*

88. Data breaches have proven to be costly for affected organizations as well, with the average cost to resolve a data breach being $4.45 million dollars in 2023.[40] The average cost to resolve a data breach involving health information, however, is more than double this figure at $10.92 million.[41]

89. 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, $13,500 to resolve problems arising from this crime), and the risk of criminal prosecution under anti-drug laws.[42]

90. 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.

91. Moreover, the temporary, non-automatic 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.

92. 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;

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

[40] *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.

[41] *Id.*

[42] *Id.*

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 where required;

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.

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

94. As a direct and proximate result of Defendant's acts and omissions in failing to protect and secure their 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.

95. 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

96. Stroup provided her Private Information to Defendant and trusted that the information would be safeguarded according to internal policies and state and federal law. Upon receipt, this Private Information was entered and stored on Defendant's network and systems.

97. Plaintiff Stroup is very careful about sharing her sensitive Private Information. Plaintiff Stroup has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

98. Plaintiff Stroup stores any documents containing her sensitive Private Information in a safe and secure location or destroys the documents. Moreover, Plaintiff Stroup diligently chooses unique usernames and passwords for her various online accounts. Had she known Defendant failed to follow basic industry security standards and failed to implement systems to protect her Private Information, she would not have provided that information to Defendant.

99. 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. According to this letter, the following categories of information were compromised: name, mailing address, date of birth, and other demographic and contact information, including emergency contact information, Social Security number, driver's license and state ID number, insurance policy and guarantor information, diagnosis and treatment information, and other information from medical or billing records.

100. 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.

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

101. 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.

102. 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.

103. Plaintiff Stroup also lost her benefit of the bargain by paying for medical services that failed to provide the data security that was promised.

104. 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.

105. Further future identity theft monitoring is reasonable and necessary for Plaintiff Stroup and such services will include future costs and expenses. And Plaintiff Stroup has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in Defendant's possession, is protected, and safeguarded from future breaches.

2. <u>Plaintiff Georgios Asimakopoulos</u>

106. Plaintiff Asimakopoulos was a patient of CVC. As requisite to receiving medical services from Defendant, Plaintiff Asimakopoulos provided his Private Information to Defendant and trusted that the information would be safeguarded according to internal policies and state and federal law. Upon receipt, this Private Information was entered and stored on Defendant's network and systems.

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

107. Plaintiff Asimakopoulos is very careful about sharing his sensitive Private Information. Plaintiff Asimakopoulos has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

108. Plaintiff Asimakopoulos stores any documents containing his sensitive Private Information in a safe and secure location or destroys the documents. Moreover, Plaintiff Asimakopoulos diligently chooses unique usernames and passwords for his various online accounts. Had he known Defendant failed to follow basic industry security standards and failed to implement systems to protect his Private Information, he would not have provided that information to Defendant.

109. Plaintiff Asimakopoulos received CVC's data breach notice. The notice informed Plaintiff Asimakopoulos that his Private Information had been improperly accessed and obtained by third parties. According to this letter, the following categories of information were compromised: name, mailing address, date of birth, and other demographic and contact information, including emergency contact information, Social Security number, driver's license and state ID number, insurance policy and guarantor information, diagnosis and treatment information, and other information from medical or billing records.

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

111. As a result of the data breach and 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. She 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.

112. 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,

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

selling, and using his private 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.

113. 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 him; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

114. Plaintiff Asimakopoulos also lost his benefit of the bargain by paying for medical services that failed to provide the data security that was promised.

115. 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.

116. Further future identity theft monitoring is reasonable and necessary for Plaintiff Asimakopoulos and such services will include future costs and expenses. And Plaintiff Asimakopoulos has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendant's possession, is protected, and safeguarded from future breaches.

3. Plaintiff Brian Hazlett

117. Plaintiff Hazlett was a patient of CVC. As requisite to receiving medical services from Defendant, Plaintiff Hazlett provided his Private Information to Defendant and trusted that the information would be safeguarded according to internal policies and state and federal law. Upon receipt, this Private Information was entered and stored on Defendant's network and systems.

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

118. Plaintiff Hazlett is very careful about sharing his sensitive Private Information. Plaintiff Hazlett has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

119. Plaintiff Hazlett stores any documents containing his sensitive Private Information in a safe and secure location or destroys the documents. Moreover, Plaintiff Hazlett diligently chooses unique usernames and passwords for his various online accounts. Had he known Defendant failed to follow basic industry security standards and failed to implement systems to protect his Private Information, he would not have provided that information to Defendant.

120. Plaintiff Hazlett received CVC's data breach notice. The notice informed Plaintiff Hazlett that his Private Information had been improperly accessed and obtained by third parties. According to this letter, the following categories of information were compromised: name, mailing address, date of birth, and other demographic and contact information, including emergency contact information, Social Security number, driver's license and state ID number, insurance policy and guarantor information, diagnosis and treatment information, and other information from medical or billing records.

121. Following the Data Breach, Plaintiff Hazlett has been the recipient of targeted phishing text messages by individuals using Private Information that was included in the Data Breach. Specifically, Plaintiff Hazlett received a message from someone posing as Navy Federal Credit Union attempting to obtain more Private Information from Plaintiff Hazlett.

122. Plaintiff Hazlett has also received dark web notifications from his CreditWise account informing him that his email address associated with Defendant has been found on the dark web.

123. As a result of the data breach and attempted phishing texts, Plaintiff Hazlett has made reasonable efforts to mitigate the impact of the data breach, including, but not limited to, researching the data breach, changing account passwords, and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud.

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

She 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.

124. As a result of the data breach, Plaintiff Hazlett 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 private information for purposes of identity theft and fraud. Plaintiff Hazlett is concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the data breach.

125. Plaintiff Hazlett 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 him; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

126. Plaintiff Hazlett also lost his benefit of the bargain by paying for medical services that failed to provide the data security that was promised.

127. Plaintiff Hazlett 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.

128. Further future identity theft monitoring is reasonable and necessary for Plaintiff Hazlett and such services will include future costs and expenses. And Plaintiff Hazlett has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendant's possession, is protected, and safeguarded from future breaches.

4. <u>Plaintiff Dode Hammack</u>

129. Plaintiff Hammack received medical care from CVC in the past. As requisite to receiving medical services from Defendant, Plaintiff Hammack provided his Private Information to Defendant and trusted that the information would be safeguarded according to

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

internal policies and state and federal law. Upon receipt, this Private Information was entered and stored on Defendant's network and systems.

130. Plaintiff Hammack is very careful about sharing his sensitive Private Information. Plaintiff Hammack has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

131. Plaintiff Hammack stores any documents containing his sensitive Private Information in a safe and secure location or destroys the documents. Moreover, Plaintiff Hammack diligently chooses unique usernames and passwords for his various online accounts. Had he known Defendant failed to follow basic industry security standards and failed to implement systems to protect his Private Information, he would not have provided that information to Defendant.

132. Plaintiff Hammack received CVC's data breach notice. The notice informed Plaintiff Hammack that his Private Information had been improperly accessed and obtained by third parties. According to this letter, the following categories of information were compromised: name, mailing address, date of birth, and other demographic and contact information, including emergency contact information, Social Security number, driver's license and state ID number, insurance policy and guarantor information, diagnosis and treatment information, and other information from medical or billing records.

133. After the Breach, Plaintiff Hammack has experienced a significant uptick in both phishing emails and text messages to his personal email and personal cell phone.

134. As a result of the data breach and the concerning increase in phishing attempts, Plaintiff Hammack 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 he otherwise would have spent on other activities, including, but not limited to, work and recreation.

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

135. As a result of the data breach, Plaintiff Hammack 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 private information for purposes of identity theft and fraud. Plaintiff Hammack is concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the data breach.

136. Plaintiff Hammack 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 him; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

137. Plaintiff Hammack also lost his benefit of the bargain by paying for medical services that failed to provide the data security that was promised.

138. Plaintiff Hammack 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.

139. Further future identity theft monitoring is reasonable and necessary for Plaintiff Hammack and such services will include future costs and expenses. And Plaintiff Hammack has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendant's possession, is protected, and safeguarded from future breaches.

5. Plaintiff Peter Fiorentino

140. Plaintiff Fiorentino was a patient of CVC. As requisite to receiving medical services from Defendant, Plaintiff Fiorentino provided his Private Information to Defendant and trusted that the information would be safeguarded according to internal policies and state and federal law. Upon receipt, this Private Information was entered and stored on Defendant's network and systems.

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

141. Plaintiff Fiorentino is very careful about sharing his sensitive Private Information. Plaintiff Fiorentino has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

142. Plaintiff Fiorentino stores any documents containing his sensitive Private Information in a safe and secure location or destroys the documents. Moreover, Plaintiff Fiorentino diligently chooses unique usernames and passwords for his various online accounts. Had he known Defendant failed to follow basic industry security standards and failed to implement systems to protect his Private Information, he would not have provided that information to Defendant.

143. Plaintiff Fiorentino received CVC's data breach notice. The notice informed Plaintiff Fiorentino that his Private Information had been improperly accessed and obtained by third parties. According to this letter, the following categories of information were compromised: name, mailing address, date of birth, and other demographic and contact information, including emergency contact information, Social Security number, driver's license and state ID number, insurance policy and guarantor information, diagnosis and treatment information, and other information from medical or billing records.

144. As a result of the data breach, Plaintiff Fiorentino 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 he otherwise would have spent on other activities, including, but not limited to, work and recreation.

145. As a result of the data breach, Plaintiff Fiorentino 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 private information for purposes of identity theft and fraud. Plaintiff

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

Fiorentino is concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the data breach.

146. Plaintiff Fiorentino 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 him; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

147. Plaintiff Fiorentino also lost his benefit of the bargain by paying for medical services that failed to provide the data security that was promised.

148. Plaintiff Fiorentino 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.

149. Further future identity theft monitoring is reasonable and necessary for Plaintiff Fiorentino and such services will include future costs and expenses. And Plaintiff Fiorentino has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendant's possession, is protected, and safeguarded from future breaches.

6. Plaintiff John Gatchell

150. Plaintiff Gatchell is a current patient of CVC, and his Private Information was and continues to be stored and maintained on CVC's computer network.

151. As a condition to receiving medical services from CVC, Plaintiff Gatchell entrusted CVC with his Private Information and reasonably expected that CVC would safeguard his Private Information in accordance with CVC's internal policies and state and federal law.

152. Plaintiff Gatchell is very careful with his Private Information. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

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

153. Plaintiff Gatchell stores any documents containing his Private Information in a safe and secure location or destroys the documents. Moreover, Plaintiff Gatchell diligently chooses unique usernames and passwords for his various online accounts. Had he known that CVC failed to implement security safeguards to adequately protect his Private Information, he would not have provided his information to CVC.

154. According to the Data Breach Notice letter Plaintiff Gatchell received from CVC, his Private Information was improperly accessed and obtained by unauthorized third parties during the Data Breach. According to the letter, the following categories of information were compromised: name, mailing address, date of birth, and other demographic and contact information, including 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 or billing records.

155. In the months after the Data Breach, Plaintiff Gatchell experienced actual fraud in the form of unauthorized charges on his debit card.

156. Plaintiff Gatchell 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.

157. Plaintiff was forced to spend multiple hours attempting to mitigate the effects of the Data Breach. He will continue to spend valuable time he otherwise would have spent on other activities, including, but not limited to, work and recreation. This is time that is lost forever and cannot be recaptured.

158. Plaintiff Gatchell suffered actual injury and damages from having his Private Information compromised in the Data Breach, including, but not limited to: (a) fraudulent charges on his debit card account; (b) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from him; (c) violation of his privacy

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

rights; and (d) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

159. Plaintiff Gatchell also suffered emotional distress that is proportional to the risk of harm and loss of privacy caused by the theft of his Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity theft and fraud. Plaintiff has also suffered anxiety about unauthorized parties viewing, using, and/or publishing information related to his Social Security number, medical records, and prescriptions.

160. Plaintiff Gatchell also lost the benefit of the bargain he made with CVC by paying for medical services that failed to provide the data security that was promised.

161. Plaintiff Gatchell anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at a present, imminent, and increased risk of identity theft and fraud in perpetuity.

162. Accordingly, future identity theft monitoring is reasonable and necessary for Plaintiff Gatchell, and such services will include future costs and expenses.

163. Plaintiff Gatchell has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS REPRESENTATION ALLEGATIONS

164. 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.

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

165. 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.

166. 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 hundreds of thousands. The U.S. Department of Health and Human Services investigation reports that nearly 500,000 individuals were impacted by Defendant's Data Breach.[43] 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.

167. 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;

[43] U.S. Department of Health and Human Services, *Cases Currently Under Investigation*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Mar. 5, 2024).

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

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 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;

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.

168. 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

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

Defendant's uniform wrongful conduct. Likewise, the relief to which Plaintiffs are entitled is typical of the Class because Defendant has acted, and refused to act, on grounds generally applicable to the Class.

169. 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.

170. 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 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.

VI. CAUSES OF ACTION

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

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

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

172. Defendant owes a duty of care to protect the Private Information belonging to Plaintiffs and Class members. Defendant's duty of care encompasses 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 maintain Plaintiffs and Class Members' Private Information in an encrypted from;

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

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

173. 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 . . . 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.

174. 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.

175. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and Class members. Plaintiffs

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

and Class members entrusted their Private Information to Defendant with the understanding that adequate security precautions would be taken to protect their information. Furthermore, only Defendant had the ability to protect its systems, and the Private Information stored on them, from attack.

176. 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.

177. 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.

178. 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.

179. 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;
- 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.

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

180. 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.

181. 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.

182. 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)

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

184. 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.

185. 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*.

186. 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.

187. 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

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

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.*

188. Defendant violated the FTCA and HIPAA by failing to implement and maintain fair, reasonable, or adequate data security practices to secure, protect, and/or otherwise safeguard Plaintiffs' and Class members' Private Information.

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

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

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

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

193. 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.

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

195. 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.

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

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

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

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

198. 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.

199. 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.

200. 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.

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

202. 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.

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

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

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

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

205. Plaintiffs and Class members conferred a monetary benefit on Defendant, by providing Defendant with their valuable Private Information. Indeed, in acquiring the Private Information, Defendant was then able to charge money for its medical services.

206. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class members' Private Information, which cost savings increased the profitability of the services.

207. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiffs and Class members by utilizing cheaper, ineffective security measures. Plaintiffs and Class members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

208. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiffs and Class members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

209. Defendant acquired the monetary benefit, PII, and PHI through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

210. Had Plaintiffs and Class members known that Defendant had not secured their PII and PHI, they would not have agreed to provide their PII and PHI to Defendant.

211. Plaintiffs and Class members have no adequate remedy at law.

212. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm.

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

213. Furthermore, as a direct and proximate result of Defendant's unreasonable and inadequate data security practices, Plaintiffs and Class members are at a current and ongoing risk of identity theft and have sustained incidental and consequential damages, including: (a) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) financial "out of pocket" costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (e) loss of time due to increased spam and targeted marketing emails; (f) the loss of benefit of the bargain (price premium damages); (g) diminution of value of their Private Information; (h) future costs of identity theft monitoring; and (i) the continued risk to their Private Information, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class members' Private Information.

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

215. 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 audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class members.

216. Moreover, Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class members overpaid for Defendant's services.

COUNT V
BREACH OF FIDUCIARY DUTY
(By Plaintiffs on behalf of the Class)

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

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

218. In light of the special relationship between Defendant and Plaintiffs and Class members, whereby Defendant became guardians of Plaintiffs' and Class members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiff and Class members: (1) for the safeguarding of Plaintiffs' and Class members' Private Information; (2) to timely notify Plaintiffs and Class members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information Defendant did and do store (and where).

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

220. Defendant breached its fiduciary duties to Plaintiffs and Class members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

221. Defendant breached its fiduciary duties to Plaintiffs and Class members by failing to encrypt or otherwise protect the integrity of the systems containing Plaintiffs' and Class members' Private Information.

222. Defendant breached its fiduciary duties to Plaintiffs and Class members by failing to timely notify and/or warn Plaintiffs and Class members of the Data Breach.

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

224. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class members sustained compensatory damages including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and

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

targeted marketing emails; (g) diminution of value of their Private Information; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance; and (j) the continued risk to their Private Information, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class members' Private Information.

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

226. 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 audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class members.

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

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

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

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

229. 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.

230. 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.

231. 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 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 FTCA, 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.

232. 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

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

personal data utilize appropriate security measures, as reflected in laws, such as HIPAA and the FTCA.

233. 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.

234. 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 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 Defendant would safeguard their data against theft and not allow access and misuse of their data by others; and

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

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 Defendant fails to undertake appropriate and adequate measures to protect data in its possession.

235. 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.

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

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

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

238. 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.

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

240. 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.

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

241. 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.

242. 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 Class members' rights to have such information kept confidential and private, by failing to provide adequate notice of the Data Breach, and by 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 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 Arizona 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 grant declaratory judgment and injunctive relief as prayed for herein;

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

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

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

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

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

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

I. 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.

RESPECTFULLY SUBMITTED this 12th day of March, 2024.

PEREZ LAW GROUP, PLLC

/s/ Cristina Perez Hesano

Cristina Perez Hesano, Esq.
7508 N. 59th Avenue
Glendale, AZ 85301
Telephone: 602.730.7100
Fax: 623.235.6173

Daniel O. Herrera *(Pro Hac Vice Forthcoming)*
Nickolas J. Hagman *(Pro Hac Vice Forthcoming)*
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

Joseph M. Lyon
(Pro Hac Vice Application forthcoming)
Kevin M. Cox
(Pro Hac Vice Forthcoming)
THE LYON FIRM
2754 Erie Ave.
Cincinnati, OH 45208
Phone: (513) 381-2333

Fax: (513) 766-9011
Email: jlyon@thelyonfirm.com
Email: kcox@thelyonfirm.com

Terence R. Coates *(Pro Hac Vice Forthcoming)*
Jonathan T. Deters *(Pro Hac Vice Forthcoming)*
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Telephone 513.651.3700
Fax 513.665.0219
tcoates@msdlegal.com
jdeters@msdlegal.com

Samuel J. Strauss *(Pro Hac Vice Forthcoming)*
Raina Borrelli *(Pro Hac Vice Forthcoming)*
Brittany Resch *(Pro Hac Vice Forthcoming)*
TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, Wisconsin 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
sam@turkestrauss.com
raina@turkestrauss.com
brittanyr@turkestrauss.com

Hart L. Robinovitch (AZ #020910)
ZIMMERMAN REED LLP
14648 N. Scottsdale Road, Suite 130
Scottsdale, AZ 85254
Telephone: (480) 348-6400
hart.robinovitch@zimmreed.com

Brian C. Gudmundson *(Pro Hac Vice Forthcoming)*
ZIMMERMAN REED LLP
1100 IDS Center, 80 S. 8th Street
Minneapolis, MN 55402
Telephone: (612) 341-0400
brian.gudmundson@zimmreed.com

James J. Pizzirusso *(Pro Hac Vice Forthcoming)*
HAUSFELD LLP
888 16th Street, N.W., Suite 300
Washington, D.C. 20006
Telephone: (202) 540-7200
Facsimile: (202) 540-7201
jpizzirusso@hausfeld.com

Steven M. Nathan *(Pro Hac Vice Forthcoming)*
HAUSFELD LLP
33 Whitehall Street, Fourteenth Floor
New York, NY 10004
Telephone: (646) 357-1100
Facsimile: (212) 202-4322
snathan@hausfeld.com

Gary F. Lynch *(Pro Hac Vice Forthcoming)*
LYNCH CARPENTER LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Telephone: (412) 322-9243
Facsimile: (412) 231-0246
gary@lcllp.com

Attorneys for Plaintiffs and the Proposed Class

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