IN THE CIRCUIT COURT OF THE STATE OF OREGON

FOR THE COUNTY OF MULTNOMAH

KIMBERLY HARVEY PERRY, individually and on behalf of all others similarly situated,

Plaintiff,

v.

AVAMERE HEALTH SERVICES, LLC,

Defendant.

Case No.

CLASS ACTION COMPLAINT

NOT SUBJECT TO MANDATORY ARBITRATION

Filing Fee: $281
Fee Authority: ORS 21.135(1), 2(a)

JURY TRIAL DEMANDED

I. INTRODUCTION

1.

Plaintiff Kimberly Harvey Perry brings this action against Defendant Avamere Health Services, LLC ("Defendant" or "Avamere") on behalf of herself and all others similarly situated to obtain equitable and injunctive relief for the Class, as defined below. Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of her counsel, and the facts that are a matter of public record. Pursuant to Oregon Rules of Civil Procedure ("ORCP") 32 J, Plaintiff presently seeks only equitable relief. Pursuant to ORCP 32 H, Plaintiff has provided notice and demand to Defendant for damages, and should Defendant not meet that demand, Plaintiff intends to amend her answer to seek damages after the expiration of the 30-day period specified.

//

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

II. NATURE OF THE ACTION

2.

This class action arises out of the recent data breach (the "Data Breach") that was perpetrated against Defendant's inadequately secured computer network, and as a result, unauthorized parties were able to have "intermittent unauthorized access" to Avamere's network between January 19, 2022 and March 17, 2022 and "potentially removed" certain files and folders from its system. See Plaintiff's Notice Letter, Exhibit A.

3.

On June 17, 2022, Avamere Health Services, LLC ("Avamere") notified certain individuals about a security incident. The Data Breach resulted in unauthorized access and exfiltration of highly sensitive and personal information.

4.

Avamere admits the "files and folders" which were removed from its system contained: "identifiable protected health information such as full names, addresses, dates of birth, driver's license or state identification numbers, Social Security numbers, claims information, financial account numbers, medications information, lab results, and medical diagnosis/conditions information."[1]

5.

The personal information compromised in the Data Breach affected individuals who are associated with a multitude of Avamere's business associates. Each of the individuals who received a belated notice of the Data Breach ("Class Members") from Avamere on behalf of the business associates has been injured by Avamere's failure to protect its computer systems from unauthorized access by cybercriminals.

//

[1] https://www.avamere.com/data-security-incident/ (last visited August 15, 2022).

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

6.

The Notice Letter was sent on behalf of a long list of entities connected with Avamere, which is a Business Associate of these entities as defined under the Health Insurance Portability and Accountability Act ("HIPPA").[2]

7.

After their investigation concluded on June 22, 2022, the Notice was amended by adding two additional entities that they discovered to be affected by the breach.[3]

8.

The protected health information related to these last two added entities included: "full names, medical diagnoses/conditions information, admit/discharge dates, and providers names related to dates of service between September 2016 through November 2021."[4]

9.

As a result of the Data Breach, certain personally identifiable information ("PII") of a broad group of individuals, including Plaintiff, was accessed and intentionally stolen. These individuals were associated with Defendant through its associated business entities.

10.

During the attack, cybercriminals stole all or some of the following PII, exclusively belonging to these individuals, between the dates January 19, 2022 and March 17, 2022: full names, addresses, dates of birth, driver's license or state identification numbers, Social Security numbers, insurance claims information, financial account numbers, medications information, lab results, and medical diagnosis/conditions information.

11.

As a result of the Data Breach, Plaintiff and Class Members suffered ascertainable

---

[2] *Id.*
[3] *Id.*
[4] *Id.*

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

losses in the form of loss of the value of their private and confidential information, loss of the benefit of their contractual bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

12.

Plaintiff's and Class Members' sensitive personal information—which was entrusted to Defendant, its officers, and agents, through its subsidiaries and associated businesses—was compromised, unlawfully accessed, and stolen due to the Data Breach.

13.

Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Plaintiff's and Class Members' Private Information that it collected and maintained.

14.

Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks of this type.

15.

Upon information and belief, the mechanism of the cyber-attack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known and foreseeable risk to Defendant, and Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

16.

In addition, Defendant and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant properly monitored its property, it would have discovered the intrusion sooner, notified the Class sooner, and

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

permitted the Class members to mitigate their own injuries.

17.

Because of the Data Breach, Plaintiff and Class Members suffered injury in the form of theft and misuse of their Private Information.

18.

In addition, Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendants collected and maintained is now in the hands of data thieves.

19.

As a further result of the Data Breach, Plaintiff and Class Members have been exposed to a substantial and present risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

20.

Plaintiff seeks remedies including, but not limited to, injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate, long-term credit monitoring and identity restoration services funded by Defendant. Plaintiff will seek to amend this Complaint after the time for her pending notice and demand expire, should Defendant fail to meet her demand.

21.

Accordingly, Plaintiff brings this action against Defendant seeking to redress its unlawful conduct.

III. PARTIES

22.

Plaintiff Kimberly Harvey Perry is a former employee of Defendant Avamere who is

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

a citizen of and resides in Central Point, Jackson County, Oregon. She received a notice letter from Defendant dated June 17, 2022. See Plaintiff's Notice Letter ("Notice Letter"), attached as Exhibit A.

23.

Avamere Health Services, LLC is a group of affiliated companies, all of which provide either skilled nursing or senior living options to residents and patients. Avamere's business is centralized in the State of Oregon although it also has facilities in Washington, Oregon, Nevada, Utah, Arizona, New Mexico, Nebraska, Colorado, and other states.

24.

Avamere's headquarters is located at 25115 SW Parkway Avenue, Wilsonville, Washington County, Oregon 97070. Its corporate policies and practices, including as related to data privacy, are established in, and emanate from the State of Oregon. Avamere can be served through its Registered Agent at National Registered Agents, Inc., 780 Commercial Street. SE, Suite 100, Salem, Oregon 97301.

IV. JURISDICTION AND VENUE

25.

This Court has jurisdiction over the parties and this case. Plaintiff Perry is a citizen and resident of Oregon. She brings this action pursuant to ORCP 32, individually and on behalf of those similarly situated who received notices of this Data Breach from Defendant, in order to protect and seek redress for the data breach victims. Plaintiff Perry is and remains a citizen and residents of the State of Oregon.

26.

This Court has subject matter jurisdiction over this action because Defendant maintains its headquarters in Oregon, and regularly conducts business in Multnomah County.

//

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

27.

This Court has personal jurisdiction over Defendant pursuant to O.R.S. 14.040 because it is a resident of the State of Oregon, operates and is incorporated in Oregon, and the computer systems implicated in this Ransomware Attack are likely located in Oregon.

28.

Venue is proper in Multnomah County under O.R.S. 14.080(2) because Defendant is a limited partnership authorized to do business in this State and is deemed to be a resident of any county where the limited partnership conducts regular, sustained business activity or has an office for the transaction of business or where any agent authorized to receive process resides. All claims alleged herein are based on Oregon law.

29.

Upon information and belief, a federal district court would be forced to decline to exercise CAFA jurisdiction over this matter, if filed in the federal courts. Pursuant to 28 U.S.C. § 1332(d)(4)(B), and based upon Avamere's headquarters, overwhelming presence, and extensive business holdings in the State of Oregon, Plaintiff believes that "two-thirds or more of the members of all proposed plaintiff classes in the aggregate, and the primary defendants, are citizens of the State of Oregon." Alternatively, the local controversy exception, 28 U.S.C. § 1332(d)(4)(A), may apply as "during the 3-year period preceding the filing of that class action, no other class action has been filed asserting the same or similar factual allegations against any of the defendants."

V. FACTUAL ALLEGATIONS

A. *Defendant*

30.

Defendant Avamere Health Services, LLC, claims that it has over 300 facilities and

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

employs more than 8,100 people and claims it has "enhanced" more than 86,500 lives.[5]

31.

Avamere Health Services, LLC is a group of affiliated companies, all of which provide either skilled nursing or senior living options to residents and patients. Avamere has facilities in 20 states, including facilities in Washington, Oregon, Nevada, Utah, Arizona, New Mexico, Nebraska and Colorado. [6]

B. ***The Data Breach***

32.

At all times relevant to this Complaint and especially during the dates affected by this Data Breach, i.e. between January 19, 2022 and March 17, 2022, Defendant was obligated to safeguard and protect the Private Information of Plaintiff and Class Members in accordance with all applicable laws.

33.

According to its Notice of Data Breach posted on its website7, cybercriminals gained access to company systems beginning on January 19, 2022. The breach lasted up to and through March 17, 2022. During this time, the cybercriminals "removed from our system contained identifiable protected health information" ("PHI"), as well as other highly sensitive personally identifiable information like names, addresses, Social Security numbers, driver's license numbers, and financial accounts ("PII"), collectively called Private Information.

34.

Defendant's investigation has "ended" then restarted, with the most recent updated notice to the U.S. Department of Health and Human Services, Office for Civil Rights ("HHS"), dated July 13, 2022, divulging that Private Information of at least 197,730

[5] https://www.avamere.com/our-story/ (last accessed August 15, 2022).
[6] *Id.*
[7] https://www.avamere.com/data-security-incident/ (last accessed August 15, 2022).

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

individuals was accessed during its Data Breach.[8]

35.

According to the HIPAA Journal, however, the number of individuals whose Private Information was breached and exfiltrated in Avamere's Data Breach may be significantly more given the number of entities that were affected. The HIPAA Journal lists 380,984 individuals as a more recent number of victims of the Data Breach.[9]

36.

Although the Data Breach was discovered at some unspecified date and Avamere knew by May 18, 2022 that extremely sensitive Private Information was "removed from [its] system," Avamere waited until July 13, 2022 (and later) to send out notices related to the Data Breach.[10]

37.

Plaintiff and Class Members' PII is likely for sale to criminals on the dark web, meaning that unauthorized parties accessed and viewed their unencrypted, unredacted information, including names, addresses, email addresses, dates of birth, Social Security numbers, bank account information, private health information, and more.

38.

The Breach occurred because Defendant failed to take reasonable measures to protect the Personal Identifiable Information it collected and stored. Among other things, Defendant failed to implement data security measures designed to prevent this release of information, despite repeated warnings to companies about the risk of cyberattacks and the highly publicized occurrence of many similar attacks in the recent past.

---

[8] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf;jsessionid=0539B986664ABD3EBADEC2203D46AE7D (last accessed August 23, 2022).

[9] https://www.hipaajournal.com/96-senior-living-and-healthcare-facilities-affected-by-avamere-data-breach/ (last accessed August 23, 2022).

[10] https://www.avamere.com/data-security-incident/ (last accessed August 23, 2022).

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

39.

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

C. ***Defendant's failings enabled the Data Breach.***

40.

Avamere acquires, collects, and stores a massive amount of protected PII, including financial information and other personally identifiable data, as well as PHI, of its patients and employees.

41.

As a condition of engaging in employment or utilizing the services that Defendant offers in its facilities, Avamere requires that individuals, including Plaintiff and Class, entrust them with highly confidential Private Information.

42.

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

43.

Furthermore, once an employee was no longer employed by Avamere, or

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

alternatively one a patient is no longer receiving services from Avamere, it had a duty to destroy the PII as soon as possible to prevent its misuse.

44.

Defendant had obligations created by industry standards, common law, and representations made to class members, to keep Class members' Private Information confidential and to protect it from unauthorized access and disclosure.

45.

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

46.

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

47.

Defendant's failure to provide adequate security measures to safeguard Private Information is especially egregious because Defendant was on notice that scammers frequently target businesses with the goal of gaining access to and exploiting Private Information.

48.

Defendant, like other health care companies, has been on notice for years that Plaintiff's and all other Class members' PII was a target for malicious actors. Despite such knowledge, Avamere failed to implement and maintain reasonable and appropriate security measures to protect Plaintiff's and Class members' PII from unauthorized access Avamere should have anticipated and guarded against.

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

D. ***Defendant was aware of data breach risks.***

49.

Businesses, including those of Defendant, are on notice that data breaches are increasingly common.

50.

Data breaches, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry, including Defendant.

51.

According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[11] Identity thieves use the stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[12]

52.

The Private Information of Plaintiff and Class members was taken by cyber criminals for the very purpose of engaging in identity theft, or to sell it to other criminals who will purchase the Private Information for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

---

[11] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013), https://www.myoccu.org/sites/default/files/pdf/taking-charge-1.pdf (last visited August 15, 2022).

[12] *Id*. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

53.

Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, especially Social Security numbers, driver's license numbers and/or state identification numbers, and of the foreseeable consequences that would occur if Defendant's data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members a result of a breach.

54.

Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. They are incurring and will continue to incur such injuries in addition to any fraudulent use of their PII.

55.

The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

E. ***Defendant failed to comply with FTC guidelines.***

56.

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

57.

In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

computer networks; understand their networks' vulnerabilities; and implement policies to correct any security problems. 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.

58.

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

59.

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

60.

Defendant failed to properly implement basic data security practices, and its failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

//

NICK KAHL
ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

61.

To prevent and detect data breaches, like the one that occurred here, Defendant could and should have implemented, as recommended by the United States Government.

62.

Although Avamere has not disclosed the exact access mechanism utilized by the cyber criminals in this Data Breach, there is at least some speculation that Avamere's networks suffered a ransomware attack.[13]

63.

To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

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

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

[13] https://www.hipaajournal.com/96-senior-living-and-healthcare-facilities-affected-by-avamere-data-breach/ (last accessed August 15, 2022).

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

instead of .net).

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

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

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

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

g. **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic.[14]

64.

Defendant was at all times fully aware of its obligation to protect the Private Information of patients, prospective patients, and employees. Defendant was also aware of the significant repercussions that would result from its failure to do so.

[14] https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited August 15, 2022).

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

F. ***Defendant failed to comply with industry standards.***

65.

A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendant's cybersecurity practices. Best cybersecurity practices include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

66.

Upon information and belief, Defendant failed to meet the minimum standards of the following cybersecurity 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 established standards in reasonable cybersecurity readiness. These frameworks are existing and applicable industry standards in Defendant's industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber-attack and causing the Data Breach.

67.

The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach.

//

//

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

G. *Defendant breached it obligations to Plaintiff and the Class.*

68.

Defendant breached its obligations to Plaintiff and Class Members and/or were otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems, networks, and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect customers' Private Information;

c. Failing to properly monitor their data security systems for existing intrusions, brute-force attempts, and clearing of event logs;

d. Failing to apply all available security updates;

e. Failing to install the latest software patches, update its firewalls, check user account privileges, or ensure proper security practices;

f. Failing to practice the principle of least-privilege and maintain credential hygiene;

g. Failing to avoid the use of domain-wide, admin-level service accounts;

h. Failing to employ or enforce the use of strong randomized, just-in-time local administrator passwords, and;

i. Failing to properly train and supervise employees in the proper handling of inbound emails.

69.

As the result of computer systems in dire need of security upgrading and inadequate procedures for handling cybersecurity threats, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

70.

Accordingly, as outlined below, Plaintiff and Class Members now face a substantial, increased, and present risk of fraud and identity theft.

71.

In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with Defendant because of its inadequate data security practices for which they gave good and valuable consideration.

H. ***Data breaches put consumers at an increased risk of fraud and identity theft.***

72.

Defendant was well aware that the Private Information it collects is highly sensitive, and of significant value to those who would use it for wrongful purposes, like the cybercriminals who perpetrated this cyber-attack.

73.

The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[15]

74.

That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. The reason criminals steal PII and PHI is to monetize it.

75.

By selling Private Information on the black market, thieves are able to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. The greater number of pieces of data and the more accurate data

[15] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, available at: https://www.gao.gov/assets/gao-07-737.pdf (last visited August 15, 2022) ("GAO Report").

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

stolen in a data breach, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim.

76.

For example, armed with just a name and date of birth, a data thief can use a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number.

77.

Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

78.

The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[16]

79.

Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud; to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

//

[16] *See* https://www.identitytheft.gov/Steps (last accessed August 15, 2022).

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

80.

In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

81.

Theft of Private Information—as occurred here—is gravely serious. PII is a valuable property right.[17] Its value is axiomatic, considering the value of big data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

82.

It must also be noted there may be a substantial time lag – measured in years – between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

83.

According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

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

See GAO Report, at 29.

[17] *See, e.g.*, John T. Soma, *et al*., Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

84.

Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

85.

There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at a substantial and immediate present risk of fraud and identity theft that will continue for many years.

86.

Thus, Plaintiff and Class Members must vigilantly monitor their financial accounts for many years to come.

87.

Sensitive Private Information can sell for as much as $363 according to the Infosec Institute. PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200.

88.

Social Security numbers are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and

extensive financial fraud.

89.

For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.

90.

Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

91.

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

92.

This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are

[18] *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Brian Naylor, Feb. 9, 2015, available at: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited August 15, 2022).

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

worth more than 10x on the black market."

93.

Driver's license numbers are also incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about $1200 on the Dark Web. On its own, a forged license can sell for around $200."[19]

94.

According to national credit bureau Experian:

> A driver's license is an identity thief's paradise. With that one card, someone knows your birthdate, address, and even your height, eye color, and signature. If someone gets your driver's license number, it is also concerning because it's connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep a copy of your driver's license on file), doctor's office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you. Next to your Social Security number, your driver's license number is one of the most important pieces of information to keep safe from thieves.

95.

According to cybersecurity specialty publication CPO Magazine, "[t]o those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation."[20] However, this is not the case. As cybersecurity experts point out:

> It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks.[21]

//

[19] https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658 (last visited August 15, 2022).
[20] https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last visited August 15, 2022).
[21] *Id.*

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

96.

Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.[22]

97.

At all relevant times, Defendant knew or reasonably should have known these risks, the importance of safeguarding Private Information, and the foreseeable consequences if its data security systems were breached, and strengthened their data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

I. *Defendant's duty to protect PHI is well-established under HIPAA.*

98.

Defendant has obligations created by HIPAA, industry standards and common law to keep Class Members' Personal Information confidential and to protect it from unauthorized access and disclosure.

99.

Defendant's data security obligations were particularly important given the substantial increase in data breaches in the healthcare industry preceding the date of the breach.

100.

Cyberattacks against hospitals and healthcare organizations such as Defendant are targeted. According to the 2019 Health Information Management Systems Society, Inc. ("HIMMS") Cybersecurity Survey, "[a] pattern of cybersecurity threats and experiences is discernable across US healthcare organizations. Significant security incidents are a near-

[22] *How Identity Thieves Took My Wife for a Ride,* NY Times, April 27, 2021, available at: https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last visited August 15, 2022).

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

universal experience in US healthcare organizations with many of the incidents initiated by bad actors, leveraging e-mail as a means to compromise the integrity of their targets."23 Healthcare facilities "have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information (PII) for thousands of patients at any given time. From social security and insurance policies to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[24]

101.

Defendant had clearly-defined and mandatory obligations created by HIPAA, contract, industry standards, common law, and representations made to Plaintiff and Class Members, to keep their Personal Information confidential and to protect it from unauthorized access and disclosure.

102.

Plaintiff and Class Members provided their Personal Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

103.

Defendant's data security obligations were particularly important given the substantial increase in data breaches, and particularly data breaches in the healthcare industry, preceding the date of the breach.

104.

Data breaches, including those perpetrated against the healthcare sector of the

[23] https://www.himss.org/himss-cybersecurity-survey (last accessed May 2, 2022).
[24] Eyal Benishti, How to Safeguard Hospital Data from Email Spoofing Attacks, Chief Healthcare Executive (April 4, 2019) at: https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last accessed May 3, 2022).

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

economy, have become widespread. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[25]

105.

Of the 1,473 recorded data breaches, 525 of them, or 35.64%, were in the medical or healthcare industry.[26] The 525 reported breaches reported in 2019 exposed nearly 40 million sensitive records (39,378,157), compared to only 369 breaches that exposed just over 10 million sensitive records (10,632,600) in 2018.[27]

106.

In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[28] Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Avamere.

107.

Cyberattacks such as the one against Avamere are especially problematic because of the disruption they cause to the daily lives of victims affected by the Data Breach.

108.

Other security experts agree that when a cyberattack occurs, a data breach does as well, because such an attack represents a loss of control of the data within a network.[29]

109.

HIPAA requires covered entities and the business associates of covered entities to

---

[25] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last accessed May 2, 2022).
[26] *Id*.
[27] *Id.* at p. 15.
[28] *See* Maria Henriquez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last accessed May 2, 2022).
[29] *See* Sung J. Choi et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019). Available at https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203 (last accessed May 2, 2022).

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

protect against reasonably anticipated threats to the security of sensitive patient health information.

110.

Defendant Avamere is a business associate of a "covered entity" under HIPAA. Business associates of covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical and administrative components.

111.

Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, et seq. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

112.

Avamere experienced a breach as defined by the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule.

113.

A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.40.

114.

Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate Avamere failed to comply with safeguards mandated by HIPAA regulations.

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

J. ***Elderly populations are reluctant to change after a data breach.***

115.

Avamere's primary business is providing healthcare and rehabilitation at senior living facilities.

116.

In 2020, the AARP sponsored Javelin Strategy Research to do a report on identity fraud strategies for Americans aged 55 years and older. While this report and its related research show that elders experience similar rates of being victims or identity fraud as the overall U.S. population, it also indicates certain troublesome patterns among this population, which includes a majority of the patients/residents at Avamere.

117.

After being a victim of identity fraud, "[c]onsumers aged 65+ typically do not change how they shop, bank, or pay following a fraudulent event. A surprising 70% of consumers 65 and older exhibit reluctance to change familiar habits." This reluctance increases the risks that elders face after a data breach like that at Avamere.

118.

For Americans 55+ years old, Javelin's research has shown that they are more likely to use identity theft protection, credit report security freezes, and credit monitoring than the overall U.S. population.

119.

Since elders are more likely to rely on the type of credit monitoring services that Avamere has offered, albeit for only one year, and because many of the victims of the Avamere Data Breach are likely to be over 55 years old, Avamere's offer of a single year of free credit is woefully inadequate. Their Personal Information is likely to be exploited for years, yet Avamere's relief is limited.

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

K. ***Plaintiff and Class Members suffered injuries.***

120.

Defendant entirely fails to provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII.

121.

Plaintiff and Class Members have been damaged by the compromise of their PII in the Data Breach.

122.

Plaintiff and Class Members presently face substantial risk of out-of-pocket fraud losses such as loans opened in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

123.

Plaintiff and Class Members have been, and currently face substantial risk of being targeted now and in the future, subjected to phishing, data intrusion, and other illegality based on their PII as potential fraudsters could use that information to target such schemes more effectively to Plaintiff and Class Members.

124.

Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

125.

Plaintiff and Class members also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in data breach cases.

//

NICK KAHL
ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

126.

Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

127.

Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

128.

Moreover, Plaintiff and Class Members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password protected.

129.

Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their PII —which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

130.

As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

//

NICK KAHL
ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

L. *Plaintiff's Experience*

131.

Plaintiff Kimberly Harvey Perry is and at all times mentioned herein is an individual citizen residing in the State of Oregon, in the City of Central Point, Jackson County.

132.

Plaintiff Perry is a former employee of Avamere Health Services, LLC. When she was initially employed by Avamere, she was required to provide Avamere with her Personal Information, including but not limited to her Social Security number.

133.

On or about June 17, 2022, Plaintiff Perry received a mailed Notice of Data Breach Letter, related to Avamere's Data Breach that occurred between January 2022 and March 2022. Attached as Exhibit A.

134.

The Notice Letter that Plaintiff Perry received listed an extensive amount of her PII and PHI that was stolen due to, "intermittent unauthorized access to a network controlled by Avamere Health Services, LLC." The letter stated that the "acquired [stolen] files" included her "Full name, Social Security number, date of birth, and medical information." *See* Exhibit A.

135.

Plaintiff Perry is alarmed by the amount of her Personal Information that was stolen or accessed, and even more by the fact that her Social Security numbers were identified as amount the breached data on Avamere's computer system.

136.

Had she known that Defendant would not take reasonable steps to safeguard her sensitive PII, Plaintiff may not have sought employment at Defendant's business, or at the

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

very least, would have insisted that Defendant take additional steps to preserve and protect her PII on its computer systems and remove all of her PII was that unnecessary for its regular employment related business transactions.

137.

Plaintiff Perry has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, which includes spending time on the telephone calls, researching the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts. This is time that has been lost forever and cannot be recaptured.

138.

For a couple of months, Plaintiff Perry has been receiving a significantly higher number of spam emails, calls, and texts. She now receives about three spam calls per a day.

139.

Since the Data Breach, Plaintiff Perry monitors her financial accounts more often. She now spends around 40 minutes a week checking her accounts for suspicious activity, which is time that she cannot spend on other activities she would prefer.

140.

Plaintiff Perry stores documents containing her PII in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for her online accounts.

141.

Plaintiff Perry has suffered actual injury in the form of injuries to, and diminution in, the value of her PII – a form of intangible property that Plaintiff entrusted to Defendant. This PII was compromised in, and has been diminished as a result of, the Data Breach.

142.

Plaintiff Perry has also suffered actual injury in the forms of lost time and opportunity

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

costs, annoyance, interference, and inconvenience as a result of the Data Breach, and has anxiety and increased concerns due to the loss of her privacy and the substantial risk of fraud and identity theft which he now faces.

143.

Plaintiff Perry has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of her PII resulting from the compromise of her PII, especially her Social Security number, in combination with her name, address, phone number, and email address, which PII is now in the hands of cyber criminals and other unauthorized third parties.

144.

Knowing that thieves stole her PII, including her Social Security number and other PII that she was required to provide to Defendant, and knowing that her PII will likely be sold on the dark web, has caused Plaintiff great anxiety.

145.

Additionally, Plaintiff Perry does not recall having been involved in any other data breaches in which this highly confidential PII was compromised.

146.

Plaintiff Perry has a continuing interest in ensuring that her PII which, upon information and belief, remains in the possession of Defendant, is protected and safeguarded from future data breaches.

147.

Due to the Data Breach, Plaintiff Perry is presently and will continue to be at a present and heightened risk for financial fraud, identity theft, other forms of fraud, and the injuries that result from such breaches, known and unknown, for years to come.

148.

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

Plaintiff reasonably believes that her Private Information has or will soon be sold on the Dark Web.

149.

As a result of the Data Breach, Plaintiff Perry already does and reasonably anticipates spending even more time and money in the future to try to mitigate and address harms caused by the Defendant's Data Breach.

VI. CLASS ACTION ALLEGATIONS

150.

Plaintiff brings this action as a representative party pursuant to ORCP 32, and on behalf of a class initially defined as:

> All persons whose Private Information was compromised as a result of the Data Breach of Defendant Avamere and occurred between approximately January 19, 2022 through March 17, 2022 (the "Class").

151.

Plaintiff reserves the right to modify or refine the Class definition based upon discovery of new information and in order to accommodate any of the Court's manageability concerns.

152.

Excluded from the class are Defendants, any entity in which Defendants have a controlling interest or that has a controlling interest in (or is under common control with) Defendants, and Defendants' legal representatives, assignees, and successors. Also excluded are the judge to whom this case is assigned and any member of the judge's immediate family.

153.

The class is so numerous, consisting of more than 100 members, that joinder of all

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

members is impracticable.

154.

There are numerous questions of fact and law common to Plaintiffs and class members. Common questions include, but are not limited to, the following:

a. Whether Defendant engaged in the activities referenced in the above paragraphs;

b. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

c. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

d. Whether Defendant properly implemented its purported security measures to protect Plaintiff's and the Class's Private Information from unauthorized capture, dissemination, and misuse;

e. Whether Defendant took reasonable measures to determine the extent of the Data Breach after it first learned of same;

f. Whether Defendant disclosed Plaintiff's and the Class's Private Information in violation of the understanding that the Private Information was being disclosed in confidence and should be maintained;

g. Whether Defendant willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and the Class's Private Information;

h. Whether Defendant was negligent in failing to properly secure and protect Plaintiff's and the Class's Private Information;

i. Whether Defendant was unjustly enriched by its actions; and

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

j. Whether Plaintiff and the other members of the Class are entitled to injunctive relief or other equitable relief, and damages (if sought in amendment), as well as the determination of such relief.

155.

Defendant engaged in a common course of conduct toward Plaintiff and members of the class. The common issues of fact and law arising from this conduct that affect Plaintiff and members of the class predominate over any individual issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

156.

Plaintiff's claims are typical of the claims of all class members. Plaintiff's claims and the claims of the class arise out of the same common course of conduct by Defendants and are based on the same legal, equitable, and remedial theories.

157.

Plaintiff fairly and adequately protects the interests of the class. Plaintiff's claims are typical of the claims of all class members. Plaintiff has retained competent and capable attorneys with experience in complex and class action litigation. Plaintiff and her counsel are committed to prosecuting this action vigorously on behalf of the class and have the financial resources to do so. Neither Plaintiff nor her counsel have interests that are contrary to or that conflict with those of the proposed class.

158.

A class action is the superior method for the fair and efficient adjudication of this controversy. Common questions of law and fact predominate over any individual questions. Class treatment is superior to multiple individual suits or piecemeal litigation because it conserves judicial resources, promotes consistency and efficiency of adjudication, provides

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

a forum for small claimants, and deters illegal activities. Individual members of the class will have little to no interest in controlling the litigation due to the high costs of individual actions and the expense and difficulty of litigating against sophisticated parties, such as Defendants. There will be no significant difficulty in the management of this case as a class action.

159.

This Court is experienced in managing class action litigation and is a desirable forum because Defendant conduct significant business in this county and in Oregon.

160.

Plaintiff reserves her right to amend the complaint to allege claims for damages and other equitable relief. Plaintiff and the class have suffered damages and are continuing to suffer damages. Pursuant to ORCP 32 H, concurrent with the filing of this Complaint, Plaintiff, through counsel, is sending Defendant a notice and demand required to commence a class action for damages. Plaintiff intends to amend the complaint to allege claims for damages as provided pursuant to ORCP 32 H. Plaintiff is not seeking to recover for personal injury on behalf of herself or the class.

161.

Plaintiff reserves her right to amend the complaint to allege claims for punitive damages.

FIRST CAUSE OF ACTION

Count 1: Common Law Negligence

162.

Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

//

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

163.

Plaintiff and Class Members entrusted Defendant with their PII and PHI as a condition of receiving employment from or receiving services from Defendant, use their PII for business purposes only, and not disclose their PII to unauthorized third parties.

164.

Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, using, and protecting their PII and PHI from unauthorized third parties.

165.

The legal duties owed by Defendant to Plaintiff and Class Members include, but are not limited to the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII of Plaintiff and Class Members in Defendant's possession;

b. To protect the PII of Plaintiff and Class Members in Defendant's possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and

c. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiff and Class members of the Data Breach.

166.

Defendant's duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a) (the "FTC Act"), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the Federal Trade Commission, the unfair practices by companies such as Defendants of failing to use reasonable measures to protect PII.

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

167.

Various FTC publications and data security breach orders further form the basis of Defendant's duty. Plaintiff and Class Members are consumers under the FTC Act. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and by not complying with industry standards.

168.

Defendant breached its duties to Plaintiff and Class Members. Defendant knew or should have known the risks of collecting and storing PII and PHI and the importance of maintaining secure systems, especially in light of the increases in data breaches in recent years.

169.

Defendant knew or should have known that its security practices did not adequately safeguard the PII and PHI of Plaintiff and Class Members.

170.

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

171.

HIPAA imposes a duty and an actionable standard of care for an ordinary negligence claim. The HIPAA Privacy Rule prohibits covered entities from using or disclosing personal health information except as permitted by regulation. 45 C.F.R. § 164.502(a). The HIPAA privacy restrictions also govern the business associates of covered entities. 45 C.F.R. § 160.102. Avamere is subject to the actionable standards of care established by HIPAA.

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

172.

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

173.

Through Defendant's acts and omissions described in this Complaint, including Defendant's failure to provide adequate security and its failure to protect the PII of Plaintiff and Class Members from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the PII of Plaintiffs and Class Members during the period it was within Defendant's possession and control.

174.

Defendant breached the duties it owes to Plaintiff and Class Members in several ways, including:

a. Failing to implement adequate security systems, protocols, and practices sufficient to protect Plaintiff's and Class Members' PII and thereby creating a foreseeable risk of harm;

b. Failing to comply with the minimum industry data security standards during the period of the Data Breach;

c. Failing to act despite knowing or having reason to know that its systems were vulnerable to attack; and

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

d. Failing to timely and accurately disclose to Plaintiff and all Class Members that their PII had been improperly acquired or accessed and was potentially available for sale to criminals on the dark web.

175.

Due to Defendant's conduct, Plaintiff and Class Members are entitled to years of credit monitoring. Credit monitoring is reasonable here. The PII taken can be used for identity theft and other types of financial fraud against them immediately and for years to come.

176.

Some experts recommend that data breach victims obtain credit monitoring services for at least ten years following a data breach. Annual subscriptions for credit monitoring plans range from approximately $219.00 to $358.00 per year.

177.

As a result of Defendant's negligence, Plaintiff and Class Members suffered injuries that may include:

a. actual identity theft;

b. the lost or diminished value of PII and PHI;

c. the compromise, publication, and/or theft of PII and PHI;

d. out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI;

e. lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including, but not limited to, time spent deleting phishing email messages and cancelling credit cards believed to be associated with the compromised account;

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

f. the continued risk to their PII and PHI, which may remain for sale on the dark web and is in Defendant's possession and subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession;

g. future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members, including ongoing credit monitoring.

178.

These injuries were reasonably foreseeable given the history of security breaches of this nature. The injury and harm that Plaintiff and Class Members suffered was the direct and proximate result of Defendant's negligent conduct.

Count 2: Negligence *Per Se*

179.

Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

180.

Pursuant to the HIPAA (42 U.S.C. § 1302d et seq.) and the FTCA, Avamere was required by law to maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiff's and Class Members' Personal Information.

181.

Avamere breached its duties by failing to employ industry standard data and cybersecurity measures to gain compliance with those laws, including, but not limited to, proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

182.

It was reasonably foreseeable, particularly given the growing number of data breaches of health information, that the failure to reasonably protect and secure Plaintiff's and Class Members' Personal Information in compliance with applicable laws would result in an unauthorized third-party gaining access to Avamere's networks, databases, and computers that stored or contained Plaintiff's and Class Members' Personal Information.

183.

Plaintiff's and Class Members' Personal Information constitutes personal property that was stolen due to Avamere's negligence, resulting in harm and injury to Plaintiff and Class Members.

184.

Avamere's conduct in violation of applicable laws directly and proximately caused the unauthorized access and disclosure of Plaintiff's and Class Members' unencrypted Personal Information.

185.

Plaintiff and Class Members have suffered and will continue to suffer as a result of Avamere's conduct. Plaintiff and Class Members seek relief as a result of Avamere's negligence.

186.

Additionally, as a direct and proximate result of Defendant's negligence per se, Plaintiff and members of the Classes have suffered and will suffer the continued risks of exposure of their PII and PHI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI in its continued possession.

//

NICK KAHL
ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

SECOND CAUSE OF ACTION

(Breach of Implied Contract)

187.

Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein, on behalf of herself and the Employee Subclass.

188.

When Plaintiff and other employee Subclass Members provided their PII and PHI to Defendant in exchange for Defendant's employment opportunities, they entered into implied contracts with Defendant under which—and by mutual assent of the parties—Defendant agreed to take reasonable steps to protect their Private Information.

189.

Defendant solicited and invited Plaintiff and Class Members to provide their PII and PHI as part of Defendant's regular business practices and as essential to the employment transactions entered into between Defendant on the one hand and Plaintiff and Class Members on the other. This conduct thus created implied contracts between Plaintiff and Class Members on the one hand, and Defendant on the other hand. Plaintiff and Class Members accepted Defendant's offers by providing their PII to Defendant in connection with their employment with Defendant.

190.

When entering into these implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws, regulations, and industry standards.

191.

Defendant's implied promise to safeguard Plaintiff and Class Members' PII and PHI is evidenced by a duty to protect and safeguard PII and PHI that Defendant required Plaintiff

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

and Class Members to provide as a condition of entering into employment relationships with Defendant.

192.

Plaintiff and Employee Subclass Members reasonably believed and expected that Defendant would use part of the funds and profits received as a result of the labor of the Plaintiff and Class Members to obtain adequate data security. Defendant failed to do so.

193.

Plaintiff and Employee Subclass Members, on the one hand, and Defendant, on the other hand, mutually intended—as inferred from Defendant's continued employment—that Defendant would adequately safeguard PII and PHI. Defendant failed to honor the parties' understanding of these contracts, causing injury to Plaintiff and Employee Subclass Members.

194.

Plaintiff and Employee Subclass Members value data security and would not have provided their PII to Defendant in the absence of Defendant's implied promise to keep the PII reasonably secure.

195.

Plaintiff and Employee Subclass Members fully performed their obligations under their implied contracts with Defendant.

196.

Defendant breached its implied contracts with Plaintiff and Employee Subclass Members by failing to implement reasonable data security measures and permitting the Data Breach to occur.

197.

As a direct and proximate result of Defendant's breaches of the implied contracts,

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

Plaintiff and Employee Subclass Members sustained injuries as alleged herein.

THIRD CAUSE OF ACTION

(Breach of Fiduciary Duty)

198.

Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

199.

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

200.

Defendant accepted the special confidence Plaintiff and class members placed in it, as evidenced by its assertion that it is committed to protecting the privacy of Plaintiff's personal information as included in the Data Breach notification letter.

201.

In light of the special relationship between Defendant and Plaintiff and class members, whereby Defendant became a guardian of Plaintiff's and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its employees or its service recipients, including Plaintiff and Class Members for the safeguarding of Plaintiff's and Class Members' Private Information.

202.

Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of its employment or service relationship, in particular, to keep

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

secure the Private Information entrusted to its care.

203.

Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to protect the integrity of the systems containing Plaintiff's and Class Member's Private Information.

204.

Defendant breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

205.

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

//

NICK KAHL
ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

206.

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

FOURTH CAUSE OF ACTION

(Unjust Enrichment)

207.

Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

208.

Defendant benefited from receiving Plaintiff's and Class members' PII by its ability to retain and use that information for its own benefit. Defendant understood this benefit.

209.

Defendant also understood and appreciated that Plaintiff's and Class Members' PII was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that PII.

210.

Plaintiff and Class Members who were employees of Defendant conferred a monetary benefit upon Defendant in the form of performing services for Defendant for which Defendant gained its profits and was able to build its business. Plaintiff and Class Members who were patients/residents who received care from Defendant and its associates conferred a monetary benefit upon Defendant in the form of payments made to Defendant for which Defendant gained its profits and was able to build its business.

211.

If Plaintiffs and Class members knew that Defendant would not secure their Private

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

Information using adequate security, they would not have agreed to release this information to Defendant.

212.

Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. Defendant also benefited from the receipt of Plaintiff and Class Members' PII, as Defendant used it to facilitate the transfer of information and payments between the parties.

213.

The monies that Plaintiff and Class Members paid to Defendant for services were to be used by Defendant, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

214.

Defendant also understood and appreciated that Plaintiff and Class Members' PII and PHI was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that PII and PHI.

215.

But for Defendant's willingness and commitment to maintain privacy and confidentiality, that PII and PHI would not have been transferred to and untrusted with Defendant. Indeed, if Defendant had informed Plaintiff and Class Members that their data and cyber security measures were inadequate, Defendant would not have been permitted to continue to operate in that fashion by regulators, its shareholders, its employees, and its patient/residents.

216.

As a result of Defendant's wrongful conduct, Defendant has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Class Members. Defendant continues to

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

benefit and profit from its retention and use of the PII while its value to Plaintiff and Class Members has been diminished.

217.

Defendant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged in this complaint, including compiling, using, and retaining Plaintiff's and Class Members' PII, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

218.

Under principals of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and Class Members that were mandated by federal, state, and local laws and industry standards.

219.

Plaintiff and Class members have no adequate remedy at law.

220.

Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiffs and Class members conferred on them.

221.

Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds it received from patient/residents, or alternatively, that it failed to spend on reasonable security measures as a part of negotiated wages for employees, as a result of the conduct alleged herein.

222.

Plaintiff is entitled to recover pre-judgment and post-judgment interest as authorized

NICK KAHL ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

by ORS 82.010.

223.

Plaintiff reserves the right to amend this complaint to add a claim for punitive damages as required by ORS 31.725.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, respectfully requests that this Court:

A. Enter an order certifying the matter as a class action pursuant to ORCP 32, appoint Plaintiff as Class representative, and appoint Plaintiff's counsel to represent the Class and Subclass;

B. Injunctive relief, enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from failing to issue prompt, complete and accurate disclosures to Plaintiff and Class and Subclass;

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

D. An order requiring an accounting with respect to the amount of damages for Plaintiff's causes of action;

E. Award other such injunctive, and declaratory relief as may be appropriate;

F. Award all costs, including experts' fees, attorneys' fees, and the costs of prosecuting this action; and

G. Grant such other legal and equitable relief as the Court may deem appropriate.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

NICK KAHL
ATTORNEY
p: 971-634-0829
f: 503-227-6840
209 SW Oak Street, Suite 400
Portland, OR 97204

Dated: August 24, 2022

Respectfully submitted,

s/ Nicholas Kahl

Nicholas A. Kahl, OSB No. 101145
NICK KAHL, LLC
209 SW Oak St., Suite 400
Portland, OR 97204
Telephone: (971) 634-0829
Facsimile: (503) 227-6840
Email: nick@nickkahl.com

-AND-

Gary E. Mason, *pro hac vice application forthcoming*
Danielle L. Perry, *pro hac vice application forthcoming*
Lisa A. White, *pro hac vice application forthcoming*
MASON LLP
5301 Wisconsin Avenue, NW
Suite 305
Washington, DC 20016
Tel: (202) 429-2290
gmason@masonllp.com
dperry@masonllp.com
lwhite@masonllp.com

Attorneys for the Plaintiff and Proposed Class

EXHIBIT A

P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:
833-909-4422
Or Visit:
https://response.idx.us/avamere
Enrollment Code:
[redacted]

105 1 32155 **********AUTO**5-DIGIT 97503
[redacted]
Kimberly Perry
[redacted]
Central Point, OR 97502
[redacted]

June 17, 2022

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

Dear Kimberly Perry:

We are writing to inform you of a data security incident involving some of your information in connection with your employment at Medford Operations, LLC. We wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your personal information.

What Happened?

We recently determined that intermittent unauthorized access to a network controlled by Avamere Health Services, LLC occurred between January 19, 2022 and March 17, 2022. Avamere Health Services, LLC provides certain information technology services to the employer(s) listed above.

What We Are Doing.

Upon learning of this issue, we immediately launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to assess the extent of any compromise. After an extensive investigation, we concluded on May 18, 2022 that an unauthorized party potentially removed a limited number of files and folders from our system that may contain your personal information.

What Information Was Involved?

The acquired files potentially contained your Full name, Social Security number, date of birth, and medical information.

What You Can Do.

To protect you from potential misuse of your information, we are offering a complimentary one year membership of identity theft protection services through IDX, a data breach and recovery services expert. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. For more information on your complimentary one year membership, please see the additional information provided in this letter.