Charles H. Thronson, USB 3260
PARSONS BEHLE & LATIMER
201 S. Main Street, Suite 1800
Salt Lake City, UT 84111
Telephone: (801) 532-1234
Facsmile: (801) 536-6111
CThronson@parsonsbehle.com

M. Anderson Berry *(pro hac vice* forthcoming)
Gregory Haroutunian (*pro hac vice* forthcoming)
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Facsimile: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com

Attorneys for Plaintiff and the Putative Class

UNITED STATES DISTRICT COURT
DISTRICT OF UTAH

JOEL THORNTON, individually and on behalf of all others similarly situated,

Plaintiff,

v.

MEDICAL REVIEW INSTITUTE OF AMERICA, LLC,

Defendant.

Case No. _____

CLASS ACTION COMPLAINT

JURY DEMAND

Plaintiff Joel Thornton ("Plaintiff"), individually and on behalf of all others similarly situated ("Class Members"), brings this Class Action Complaint against Medical Review Institute of America, LLC ("MRIoA" or "Defendant"), and alleges upon personal knowledge as to his own actions and the investigation of his counsel, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiff brings this Class Action Complaint against Defendant for its failure to adequately secure and safeguard electronically stored, personally identifiable information ("PII") and protected health information ("PHI") that Defendant collected and maintained (collectively the "Private Information"). Defendant collected and maintained, and then allowed unauthorized third persons access to, an extraordinary amount of sensitive PHI and PII, including, without limitation: Social Security number, first and last names, home address, telephone number, email addresses, date of birth, medical history, diagnoses, treatment information, dates of service, lab test results, prescription information, provider names, medical account information, financial information, health insurance policy and group plan numbers, and claim information.

2. Defendant MRIoA, based in Salt Lake City, Utah, advertises itself as "the top medical review company in the United States" and states that it "takes the privacy and security of your information very seriously."[1]

3. As a result of its business, Defendant maintains sensitive medical details and other personal information about individuals even if the individuals have not had direct relationships with MRIoA.

4. Individuals entrust Defendant, or the companies that do business with Defendant, with an extensive amount of their sensitive PII and PHI. Defendant makes public statements that they understand the importance of protecting such information. For example, in its website Privacy Policy, Defendant represents that it "take[s] your privacy very seriously," and further represents

[1] *See* https://www.ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Mar. 16, 2022) (showing two separate "Hacking" breach reports in January 2022 totaling 136,977 individuals impacted).

that "[t]he security of your Data is important to us."[2] Defendant further claims: "We have implemented procedures designed to limit the dissemination of your Data **to only such designated staff as are reasonably necessary** to carry out the stated purposes we have communicated to you."[3] But Defendant's procedures, and its promises, were not adequate: Plaintiff's and Class Member's PII and PHI ended up in the hands of criminals.

5. Despite these proclamations, however, on or before November 9, 2021, Defendant learned that an unauthorized actor breached its system and accessed and acquired electronic files containing the PHI and PII of Defendant's patients, as detailed above, including Plaintiff's and Class Members' data (the "Data Breach").

6. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PHI and PII, Defendant assumed legal and equitable duties to those individuals.

7. This PHI and PII was compromised due to Defendant's negligent, careless, and intentional acts and omissions and the failure to protect the PHI and PII of Plaintiff and Class Members.

8. Plaintiff brings this action on behalf of all persons whose PHI and PII was compromised as a result of Defendant's failure to: (i) adequately protect the PHI and PII of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of their inadequate information security practices; and (iii) avoid sharing the PHI and PII of Plaintiff and Class Members without adequate safeguards. Defendant's conduct amounts to negligence and violates federal and state statutes.

9. Plaintiff and Class Members have suffered concrete injury as a result of Defendant's conduct. These injuries include: (i) fraudulent misuse of the stolen PHI and PII that

[2] *See* https://www.mrioa.com/privacy/ (last visited Mar. 17, 2022).
[3] *Id*. (emphasis added).

is fairly traceable to this Data Breach; (ii) lost or diminished value of PHI and PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PHI and PII; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and (v) the present and immediate risk to their PHI and PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up 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 PHI and PII.

10. 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's and Class Members' PHI and 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 PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized criminal third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

PARTIES

11. Plaintiff Joel Thornton is a resident and citizen of Bradenton, Florida. Plaintiff Thornton is acting on his own behalf and on behalf of others similarly situated. Defendant obtained and continues to maintain Plaintiff Thornton's PHI and PII, including his Social Security number, and has a legal duty and obligation to protect that PHI and PII from unauthorized access and

disclosure. Plaintiff Thornton would not have entrusted his PHI and PII to Defendant had he known that it would fail to maintain adequate data security. Plaintiff Thornton's PHI and PII was compromised and disclosed as a result of the Data Breach.

12. Defendant Medical Review Institute of America, LLC, is a domestic corporation organized under the laws of the State of Utah with its principal place of business located at 2875 South Decker Lake Drive Suite 300, Salt Lake City, Utah 84119. At least one of the members of the LLC, William W. Low, is a resident of the state of Utah.

13. All of Plaintiff's claims stated herein are asserted against Defendant and any of their owners, predecessors, successors, subsidiaries, agents and/or assigns.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d)(2) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant. Plaintiff is a citizen of Florida and therefore diverse from Defendant, which is headquartered in Utah.

15. This Court has personal jurisdiction over Defendant because Defendant has its principal place of business within this District.

16. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because Defendant MRIoA headquarters are located in this District and it conducts much of its business through this District.

FACTUAL ALLEGATIONS

Background

17. Defendant MRIoA provides external review of medical, dental, behavioral health, pharmacy, vision, disability, workers' compensation, and auto claims for insurance carriers, employers, TPAs, self-administered union groups, pharmacy benefit managers, human resource consultants and departments of insurance throughout the country.[4]

18. MRIoA uses a nationwide network of board-certified physician specialists and professionals in over 133 specialties and sub-specialties of medicine. MRIoA has reviewers in most states and has licensed physicians in 50 states.[5]

19. On information and belief, in the ordinary course of business, Defendant collects from its customers (including entities to which Plaintiff and Class Members supplied their PHI and PII) sensitive personal and private information such as:

- Demographic information (i.e., first and last name, home address, phone number, email address, and date of birth);
- Social Security number;
- Clinical information (i.e., medical history/diagnosis/treatment, dates of service, lab test results, prescription information, provider name, medical account number, or anything similar in a medical file and/or record); and
- Financial information.

20. Defendant also maintains health insurance information (*i.e.*, health insurance policy

[4] *See* https://www.mrioa.com/about-us/ (last visited Mar. 16, 2022).
[5] *See* https://www.linkedin.com/company/medical-review-institute-of-america-llc (last visited Mar. 16, 2022);

and group plan number, group plan provider, claim information) relating to members of its customers' plans, including Plaintiff and Class Members

21. Plaintiff and Class Members relied on this sophisticated Defendant to keep their PHI and PII confidential and securely maintained, to use this information for business and/or medical purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their sensitive PHI and PII.

22. Defendant had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PHI and PII from involuntary disclosure to third parties.

The Data Breach

23. On November 9, 2021, MRIoA learned that it was the victim of a sophisticated cyber-attack.[6] After discovering the incident, MRIoA commenced an investigation to determine the full nature and scope of the incident and to secure its network. It also contacted the FBI to inform them of the incident.[7]

24. On November 12, 2021, MRIoA found out that the incident involved the unauthorized acquisition of information.[8] The investigation revealed that the PHI and PII was accessed without authorization, including Social Security numbers and health and financial information, and was not encrypted.[9]

---

[6] *See* https://oag.ca.gov/system/files/MRIOA%20Ad%20CM%20MRIOA%201Y%20Individual%20r2prf_1.pdf (last visited Mar. 16, 2022).

[7] *Id*.

[8] *Id*.

[9] *Id*. It is clear that the data exposed in the Data Breach was not encrypted: California law requires entities to notify California residents "whose **unencrypted personal information** was, or is reasonably believed to have been, acquired by an unauthorized person" due to a "breach of the security of the system[.]" Cal. Civ. Code § 1798.82(a)(1) (emphasis added). Defendant

25. Upon information and belief, the Data Breach targeted MRIoA due to its status as a business associate of healthcare entities and health insurance companies that collect, create, and maintain both PII and PHI. Moreover, the targeted Data Breach was expressly designed to gain access to private and confidential data, including (among other things) the PII and PHI of Plaintiff and the Class Members. Because of the Data Breach, data thieves were able to gain access to Defendant's IT systems and to access and acquire the unencrypted PHI and PII of Plaintiff and Class Members.

26. In the notices that MRIoA provided to impacted persons and the states Attorneys General, MRIoA openly admits that the PHI and PII of Plaintiff and Class Members that was accessed without authorization by hackers was indeed "acquired" by the hackers who perpetrated the Data Breach.[10] This means that not only did the cybercriminals view and access the PHI and PII without authorization, but they also removed Plaintiff's and Class Members' PHI and PII from MRIoA's network.

27. Due to MRIoA's inadequate and insufficient data security measures, Plaintiff and the Class Members now face an increased risk of fraud and identity theft and must deal with that threat forever. Plaintiff believes his PHI and PII was both stolen in the Data Breach (a fact admitted by MRIoA in its Notice of Data Breach where MRIoA states that the cybercriminals "acquired" the data) and is still in the hands of the hackers. Plaintiff further believes his PHI and PII was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals who perpetrate cyberattacks of the type that occurred here.

---

notified residents and the California Attorney General of the Data Breach on or about Feb. 3, 2022, evidencing that the exposed data was unencrypted.

[10] *Id*.

28. Defendant had obligations created by HIPAA, contract, industry standards, common law, and its customers' promises and representations made to Plaintiff and Class Members to keep their PHI and PII confidential and to protect it from unauthorized access and disclosure.

29. Plaintiff and Class Members provided their PHI and PII 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.

30. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry preceding the date of the breach.

31. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[11] Of the 1,862 recorded data breaches, 330 of them, or 17.7% were in the medical or healthcare industry.[12] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[13]

32. Indeed, cyberattacks 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. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals… because they often have

[11] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (*available at*: https://notified.idtheftcenter.org/s/), at 6.
[12] *Id.*
[13] *Id.*

lesser IT defenses and a high incentive to regain access to their data quickly."[14]

33. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in the Defendant's industry, including Defendant.

Defendant Did Not Use Reasonable Security Procedures

34. Despite this knowledge, Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, non-encrypted information it was maintaining for Plaintiff and Class Members, causing their PHI and PII to be exposed.

35. To prevent and detect cyber-attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

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

[14] FBI, Secret Service Warn of Targeted, Law360 (Nov. 18, 2019), *available at*: https://www.law360.com/articles/1220974/fbi- secret-service-warn-of-targeted-ransomware (last visited Mar. 16, 2022).

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

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

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

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

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

36. To prevent and detect cyber-attacks Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

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

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[15]

37. To prevent and detect cyber-attacks attacks Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

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

[15] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at:* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited March 17, 2022).

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[16]

38. Given that Defendant was storing the PHI and PII of Plaintiff and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect cyber-attacks.

39. 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

[16] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited March 17, 2022).

Breach and the exposure of the PHI and PII of an undisclosed amount of current and former consumers, including Plaintiff and Class Members.

Securing PII and Preventing Breaches

40. Defendant could have prevented this Data Breach by properly securing and encrypting the PHI and PII of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the data that was no longer useful, especially outdated data.

41. Defendant's negligence in safeguarding the PHI and PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to businesses to protect and secure sensitive data.

42. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

Defendant Failed to Comply with FTC Guidelines

43. The Federal Trade Commission ("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.

44. 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 computer networks; understand their network's vulnerabilities; and implement policies to correct any

security problems.[17] 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.[18]

45. 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.

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

47. Defendant failed to properly implement basic data security practices.

48. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

49. Defendant was at all times fully aware of its obligation to protect the PII of Plaintiff

[17] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited March 17, 2022).
[18] *Id.*

and Class Members. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Failed to Comply with Industry Standards

50. Several best practices have been identified that at a minimum should be implemented by companies like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data, and; limiting which employees can access sensitive data. Defendant failed to follow these industry best practices.

51. Other best cybersecurity practices that are standard in the lead exchange industry 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; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

52. Defendant failed to meet the minimum standards of any 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.

53. These foregoing frameworks are existing and applicable industry standards in the

healthcare industry, and Defendant failed to comply with these accepted standards thereby opening the door to the cyber incident and causing the data breach.

Value of Personally Identifiable Information

54. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[19] 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."[20]

55. The PII of individuals 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, and bank details have a price range of $50 to $200.[21] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[22] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[23]

56. Social Security numbers, for example, are among the worst kind of PII to have

[19] 17 C.F.R. § 248.201 (2013).
[20] *Id*.
[21] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Mar. 17, 2022).
[22] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Mar. 17, 2022).
[23] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Mar. 17, 2022).

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:

> 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.[24]

57. What is more, it is no 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. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

58. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[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."[25]

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

---

[24] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Mar. 17, 2022).

[25] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited March 17, 2022).

compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number, driver's license number, addresses, and financial information.

60. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[26]

61. Among other forms of fraud, identity thieves may use Social Security numbers to obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

62. 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."[27]

63. 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.

---

[26] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited March 17, 2022).

[27] *See* https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658 (last accessed March 17, 2022).

> 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.[28]

64. 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."[29] 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.[30]

65. Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.[31]

66. The fraudulent activity resulting from the Data Breach may not come to light for years.

67. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), 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

---

[28] Sue Poremba, *What Should I Do If My Driver's License Number is Stolen?"* (October 24, 2018) https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/ (last accessed March 17, 2022).
[29] *See* https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last accessed March 17, 2022).
[30] *Id.*
[31] *How Identity Thieves Took My Wife for a Ride,* NY Times, April 27, 2021 https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last visited Mar. 17, 2022).

> 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.[32]

68. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including Social Security numbers, driver's license numbers, and financial account information, and of the foreseeable consequences that would occur if Defendant's data security system and network was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

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

70. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to potentially thousands of individuals' detailed PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

71. 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.

72. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers and financial information, fraudulent use of that information and damage to victims may continue for

[32] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited Mar. 17, 2022).

years.

Plaintiff Joel Thornton's Experience

73. Plaintiff Thornton provided his PHI to his healthcare providers to obtain medical services in or about July 2021.

74. On or about January 7, 2022, Plaintiff Thornton received notice from Defendant that his PHI and PII had been improperly accessed by unauthorized third parties. This notice indicated that Plaintiff Thornton's PHI and PII, including full name, home address, phone number, email address, date of birth, Social Security number, medical history, diagnoses, treatment information, dates of service, lab test results, prescription information, provider names, medical account information, financial information, health insurance policy and group plan numbers, and claim information, was compromised as a result of the Data Breach.

75. Following the Data Breach, Plaintiff Thornton has experienced a substantial uptick in the number and frequency of medical-related spam mail to his home address; the same address that was supplied to Defendant.

76. Plaintiff Thornton made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach; reviewing credit reports, credit monitoring, and financial account statements for any indications of actual or attempted identity theft or fraud; researching credit monitoring and identity theft protection services offered by Defendant, and dealing with unwanted spam mail. Plaintiff Thornton has spent at least 10 hours dealing with the Data Breach, valuable time Plaintiff Thornton otherwise would have spent on other activities, including but not limited to recreation.

77. As a result of the Data Breach, Plaintiff Thornton has suffered emotional distress due to the release of his PHI, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PHI for purposes of identity theft and fraud. Plaintiff Thornton is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

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

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

CLASS ALLEGATIONS

80. Plaintiff brings this suit on behalf of himself and a class of similarly situated individuals under Federal Rule of Civil Procedure 23, which is preliminarily defined as:

> **All persons whose Private Information was maintained on MRIoA's system that was compromised in the Data Breach and who were sent a notice of the Data Breach (the "Class").**

81. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded

from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

82. Plaintiff reserves the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

83. This action is brought and may be maintained as a class action because there is a well-defined community of interest among many persons who comprise a readily ascertainable class. A well-defined community of interest exists to warrant class wide relief because Plaintiff and all members of the Classes were subjected to the same wrongful practices by Defendant, entitling them to the same relief.

84. **Numerosity.** The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, public news reports indicate that approximately 940,000 individuals had their PHI and PII compromised in this Data Breach. The identities of Class Members are ascertainable through Defendant's records, Class Members' records, publication notice, self-identification, and other means.

85. **Commonality.** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether and to what extent Defendant had a duty to protect the PHI and PII of Plaintiff and Class Members;

b. Whether Defendant had a duty not to disclose the PHI and PII of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had a duty not to use the PHI and PII of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PHI and PII Plaintiff and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PHI and PII had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PHI and PII had been compromised;

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

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PHI and PII of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual damages, nominal damages, and/or statutory damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

86. **Typicality.** Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class member, was compromised in the Data Breach.

87. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in litigating Class actions, including data privacy litigation of this kind.

88. **Predominance.** Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

89. **Superiority.** A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each

Class member.

90. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

91. Likewise, particular issues under Federal Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PHI and PII;

b. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

c. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

d. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PHI and PII; and

e. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the data breach.

92. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

93. Plaintiff and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 92.

94. Defendant knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' PHI and PII, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

95. Defendant had a duty under common law to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' PHI and PII.

96. Defendant had full knowledge of the sensitivity of the PHI and PII and the types of harm that Plaintiff and Class Members could and would suffer if the data were wrongfully disclosed.

97. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' PHI and PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

98. 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.

99. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or Class Members.

100. A breach of security, unauthorized access, and resulting injury to Plaintiff and Class Members was reasonably foreseeable, particularly in light of Defendant's inadequate security practices, including sharing and/or storing the PHI and PII of Plaintiff and Class Members on its computer systems.

101. Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PHI and PII of Plaintiff and Class Members, the critical importance of providing adequate security of that data, and the necessity for encrypting all data stored on Defendant's systems.

102. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendant's misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included their decisions not to comply with industry standards for the safekeeping of the PHI and PII of Plaintiff and Class Members, including basic encryption techniques freely available to Defendant.

103. Plaintiff and Class Members had no ability to protect their PHI and PII that was in, and possibly remains in, Defendant's possession.

104. Defendant was in a position to protect against the harm suffered by Plaintiff and

Class Members as a result of the Data Breach.

105. Defendant had and continues to have a duty to adequately disclose that the PHI and PII of Plaintiff and Class Members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PHI and PII by third parties.

106. Defendant had a duty to comply with the industry standards set out above.

107. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' PHI and PII within Defendant's possession.

108. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' PHI and PII.

109. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and Class Members that the PHI and PII within Defendant's possession might have been compromised and precisely the type of information compromised.

110. Defendant's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' PHI and PII to be compromised.

111. As a result of Defendant's ongoing failure to notify Plaintiff and Class Members regarding the type of PHI and PII has been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

112. Defendant's breaches of duty caused Plaintiff and Class Members to suffer from identity theft, fraud, loss of time and money to monitor their finances for fraud, and loss of control over their PHI and PII.

113. As a result of Defendant's negligence and breach of duties, Plaintiff and Class Members are in danger of imminent harm in that their PHI and PII, which is still in the possession of third parties, will be used for fraudulent purposes.

114. There is a close causal connection between Defendant's failure to implement security measures to protect the PHI and PII of Plaintiff and Class Members and the harm, or risk of imminent harm, suffered by Plaintiff and Class Members. The PHI and PII of Plaintiff and Class Members was stolen and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PHI and PII, by adopting, implementing, and maintaining appropriate security measures.

115. Plaintiff seeks the award of actual damages on behalf of himself and the Class.

116. In failing to secure Plaintiff's and Class Members' PHI and PII and promptly notifying them of the Data Breach, Defendant is guilty of oppression, fraud, or malice, in that Defendant acted or failed to act with a willful and conscious disregard of Plaintiff's and Class Members' rights. Plaintiff, therefore, in addition to seeking actual damages, seeks punitive damages on behalf of himself and the Class.

117. Plaintiff seeks injunctive relief on behalf of the Class in the form of an order compelling Defendant to institute appropriate data collection and safeguarding methods and policies with regard to customer information.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

118. Plaintiff and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 92.

119. Through their course of conduct, Defendant, Plaintiff, and Class Members entered into implied contracts for the Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PHI and PII.

120. Defendant induced Plaintiff and Class Members to provide and entrust their PHI and PII, including name, including, without limitation: Social Security number, first and last names, home address, telephone number, email addresses, date of birth, medical history, diagnoses, treatment information, dates of service, lab test results, prescription information, provider names, medical account information, financial information, health insurance policy and group plan numbers, and claim information.

121. Defendant solicited and invited Plaintiff and Class Members to provide their PHI and PII as part of its regular business practices. Plaintiff and Class Members accepted Defendant's offer and provided their PHI and PII to Defendant.

122. As a condition of being customers of Defendant, Plaintiff and Class Members provided and entrusted their PHI and PII to Defendant. In so doing, Plaintiff and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such non-public information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and Class Members if their data had been breached and compromised or stolen.

123. A meeting of the minds occurred when Plaintiff and Class Members agreed to, and did, provide their PHI and PII to Defendant, in exchange for, amongst other things, the protection of their Private Information.

124. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

125. Defendant breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect their PHI and PII, and by failing to provide timely and accurate notice to them that their PHI and PII was compromised as a result of the Data Breach.

126. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and Class Members have suffered (and will continue to suffer), ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

127. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and Class Members sustained damages as alleged herein.

128. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach, including the loss of the benefit of the bargain.

COUNT III
Invasion of Privacy
(On Behalf of Plaintiff and the Class)

129. Plaintiff and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 92.

130. Plaintiff and Class Members had a legitimate expectation of privacy to their PHI and PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

131. Defendant owed a duty to Plaintiff and Class Members to keep their PHI and PII confidential.

132. Defendant intentionally failed to protect and released to unknown and unauthorized third parties the non-redacted and non-encrypted PHI and PII of Plaintiff and Class Members.

133. Defendant allowed unauthorized and unknown third parties access to and examination of the PHI and PII of Plaintiff and Class Members, by way of Defendant's failure to protect the PII.

134. The unauthorized release to, custody of, and examination by unauthorized third parties of the PHI and PII of Plaintiff and Class Members is highly offensive to a reasonable person.

135. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class Members disclosed their PHI and PII to Defendant as part of their relationships with Defendant, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed

without their authorization.

136. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff's and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

137. Defendant acted with intention and a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

138. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and Class Members.

139. As a proximate result of the above acts and omissions of Defendant, the PHI and PII of Plaintiff and Class Members was disclosed to third parties without authorization, causing Plaintiff and Class Members to suffer damages.

140. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that the PHI and PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and Class Members.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

141. Plaintiff and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 92.

142. This count is plead in the alternative to the breach of implied contract count above.

143. Plaintiff and Class Members conferred a monetary benefit to Defendant when they provided their PHI and PII to receive Defendant's services.

144. Defendant knew that Plaintiff and Class Members conferred a monetary benefit to Defendant when it accepted and retained that benefit. Defendant profited from this monetary benefit, as the transmission of PHI and PII to those companies to whom Defendant makes service referrals is an integral part of Defendant's business. Without transmitting Plaintiff's and Class Members' PHI and PII to third-parties, Defendant would have dramatically diminished business and profits.

145. Defendant was supposed to use some of the monetary benefit provided to it from Plaintiff and Class Members to secure the PHI and PII belonging to Plaintiff and Class Members by paying for costs of adequate data management and security.

146. Defendant should not be permitted to retain any monetary benefit belonging to Plaintiff and Class Members because Defendant failed to implement necessary security measures to protect the PHI and PII of Plaintiff and Class Members.

147. Defendant gained access to the Plaintiff's and Class Members' PHI and PII through inequitable means because Defendant failed to disclose that it used inadequate security measures.

148. Plaintiff and Class Members were unaware of the inadequate security measures and would not have provided their PHI and PII to Defendant had they known of the inadequate security measures.

149. To the extent that this cause of action is pled in the alternative to the others, Plaintiff and Class Members have no adequate remedy at law.

150. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PHI and PII is used; (iii) the compromise and/or theft of their PHI and PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PHI and PII; (v) 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 tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PHI and PII, which remain 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 PHI and PII of Plaintiff and Class Members; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PHI and PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

151. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including,

but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

152. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds from the monetary benefit that it unjustly received from them.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class, and appointing Plaintiff and his Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PHI and PII of Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying

information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PHI and PII of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the PHI and PII of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that

includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals

must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, nominal, statutory, consequential, and punitive damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: March 18, 2022

Respectfully Submitted,

/s/ Charles H. Thronson
Charles H. Thronson, USB 3260
PARSONS BEHLE & LATIMER
201 S. Main Street, Suite 1800
Salt Lake City, UT 84111
Telephone: (801) 532-1234
Facsmile: (801) 536-6111
CThronson@parsonsbehle.com

M. Anderson Berry (*pro hac vice* forthcoming)
Gregory Haroutunian (*pro hac vice* forthcoming)
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Facsimile: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com

Attorneys for Plaintiff and the Putative Class