UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON

CYNTHIA STRECKER, individually and on behalf of all others similarly situated, Plaintiff, v. MCG HEALTH, LLC, a Washington limited liability company, Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Cynthia Strecker ("Plaintiff"), on behalf of herself and all others similarly situated, brings this action against Defendant MCG Health, LLC ("MCG Health" or "Defendant"), a Washington limited liability company, to obtain damages, restitution and injunctive relief for the Class, as defined below, from Defendant.

NATURE OF THE ACTION

1. According to a June 10, 2022 notification letter MCG sent to Plaintiff, MCG's data incident (the "Data Breach") was discovered on March 25, 2022 due to an unauthorized party obtaining certain personal information of its customers' patients and members that matched

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

data stored on Defendant's systems. The affected patient and/or member data included some or all of the following data elements: names, Social Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth and gender, hereinafter defined as personally identifiable information ("PII").

2. MCG then investigated the Data Breach and discovered that an unauthorized party may have acquired Plaintiff and approximately 1,100,000 Class Members' PII.

3. The full extent of the types of PII, the scope of the breach, and the root cause of the Data Breach are all within the exclusive control of Defendant and its agents, counsel, and forensic security vendors at this phase of the litigation.

4. Moreover, after learning of the Data Breach, Defendant waited roughly three months to notify Plaintiff and Class Members of the Data Breach and/or inform them that their PII was compromised. During this time, Plaintiff and Class Members were unaware that their sensitive personal identifying information had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm.

5. As part of its services, MCG required its customers and their patients, including Plaintiff and Class Members, to provide MCG with their PII. Defendant received Plaintiff and Class Members' PII from Plaintiff and Class Members' medical providers.

6. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals, and knew or should have known that it was responsible for safeguarding and protecting Plaintiff's and Class Members' PII from unauthorized access, disclosure, and theft due to criminal hacking activity.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

7. In acquiring and maintaining Plaintiff's and Class Members' PII, Defendant expressly and impliedly promised to safeguard Plaintiff's and Class Members' PII.

8. Upon information and belief, Defendant is responsible for allowing this Data Breach because of multiple acts of negligence, including but not limited to its: failure to design, implement, and maintain reasonable and adequate data security systems and safeguards, including but not limited to a lack of encryption; and or its failure to exercise reasonable care in the hiring, supervision, and training of its employees and agents and vendors; and/or its failure to comply with industry-standard data security practices; and/or its failure to comply with state and federal laws and regulations that govern data security and practices and are intended to protect the type of PII at issue in this action.

9. In this era of frequent data security attacks and data breaches, particularly in the medical industry, Defendant's failure leading to the Data Breach are particularly egregious, as this Data Breach was highly foreseeable.

10. Criminal hackers obtained Plaintiff's and Class Members' PII because of its value in exploiting and stealing the identities of Plaintiff and the Class Members.

11. As a direct and proximate result of the Data Breach, Plaintiff and Class Members are now at a significant present and future risk of identity theft, financial fraud, and/or other identity-theft or fraud, imminently and for years to come.

12. As a direct and proximate result of Defendant's data security failures and the Data Breach, Plaintiff and Class Members have suffered actual, concrete, and imminent injuries. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; and (iv) the continued and certainly increased risk to their 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 PII; (v) the invasion of privacy; (vi) the compromise, disclosure, theft, and unauthorized use of Plaintiff's and the Class Member's PII; and (vii) emotional distress, fear, anxiety, nuisance and annoyance related to the theft and compromise of their PII.

13. Plaintiff and Class Members seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and remains at risk due to inadequate data security.

14. 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.

15. Accordingly, Plaintiff, individually and on behalf of other Class Members, asserts claims for Negligence (Count I) and Violation of The Washington Consumer Protection (Count II).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

PARTIES

16. Plaintiff Cynthia Strecker is, and at all times mentioned herein was, an individual citizen Slidell, Louisiana. Plaintiff received a data breach notification letter dated June 10, 2022. She received medical care from Ochsner Health Care System.

17. MCG is a HIPAA business associate that provides patient care guidelines to health care providers and health plans. MCG Health, LLC is a Washington Limited Liability Company with a principal place of business at 901 5th Avenue, Suite 120, Seattle, WA 98164. MCG Health, LLC's sole member is Hearst Healthcare Holding I, Inc., located 1301 Fifth Avenue, Suite 3800, WA 98101, and as such is a citizen of the state of Washington.

JURISDICTION AND VENUE

18. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because Plaintiff and at least one member of the putative Class, as defined below, are citizens of a different state than Defendant MCG, there are more than 100 putative class members, and the amount in controversy exceeds $5 million exclusive of interest and costs. For example, Plaintiff is a citizen of Louisiana and MCG's sole member is a citizen of Washington.

19. The Western District of Washington has general personal jurisdiction over Defendant named in this action because Defendant and/or its parents or affiliates are headquartered in this District and Defendant conducts substantial business in Washington and this District through its headquarters, offices, parents, and affiliates.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

20. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

DEFENDANT'S BUSINESS

21. Defendant requires Plaintiff and Class Members or the healthcare networks that Plaintiff and Class Members use to provide the following PII: names, Social Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth and gender.

22. Before receiving Defendant's services, Plaintiff and Class Members and/or their healthcare providers were required to and did in fact turn over much (if not all) of the private and confidential information listed above.

23. Due to the highly sensitive and personal nature of the information MCG acquires and stores with respect to its patients, MCG recognizes privacy rights, and promises in its Privacy Notice, to, among other things, maintain the privacy of patients' protected health information, which includes the types of data compromised in this Data Breach.

24. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from unauthorized disclosure.

25. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

26. Plaintiff and the Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business and health purposes only, and to make only authorized disclosures of this information.

THE DATA BREACH

27. MCG realized the Data Breach on March 25, 2022. Through the Data Breach, an unauthorized party gained access to Plaintiff's and Class Members' PII stored on Defendant's systems.

28. Defendant Data Breach notification letters admitted that "an unauthorized party previously obtained certain of your personal information that matched data stored on [Defendant's] systems. The affected patient or member data included some or all of the following data elements: names, Social Security numbers, medical codes, postal addresses, telephone numbers, email addresses, dates of birth, and gender."[1]

29. On information and belief, the PII accessed was unencrypted.

30. On information and belief, the cybercriminals did in fact access Defendant's files, and exfiltrate Plaintiff's and Class Members' PII during the roughly two weeks in which the cybercriminals had unfettered access to Defendant's email network.

31. On information and belief, the targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the PII of patients and/or members, like Plaintiff and the Class Members.

[1] https://www.mcg.com/wp-content/uploads/2022/06/MCG-Website-Notice_90273447_1-6.8.22481312.4-004.pdf (last visited on June 17, 2022).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

32. While Defendant stated in notice letters sent to Plaintiff and Class Members (as well as on its website) that it learned of the Data Breach in March 2022, Defendant did not begin notifying impacted patients, such as Plaintiff and Class Members, until June 10, 2022– almost three months after discovering the Data Breach.

33. According to MCG's reporting to the Maine Attorney General about the Data Breach, the PII of roughly 1.1 million individuals, including Plaintiff, was compromised.

34. Acknowledging that its cybersecurity was deficient at the time of the Data Breach, admitted in its Data Breach notification letters that it "deployed additional monitoring tools and will continue to enhance the security of [its] systems."

35. Due to Defendant's inadequate security measures, Plaintiff and the Class Members now face a present, immediate, and ongoing risk of fraud and identity theft and must deal with that threat forever.

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

37. Plaintiff and Class Members provided their 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.

THE DATA BREACH WAS FORSEEABLE

38. Defendant's 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.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

39. To prevent and detect cyberattacks and/or ransomware 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.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

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.

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

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

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

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

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

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[2]

41. To prevent and detect cyber-attacks or ransomware 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;
> **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; and,
> - Turn on attack surface reduction rules and [Antimalware Scan Interface] for

[2] *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 June 17, 2022).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Office [Visual Basic for Applications].[3]

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

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

MCG ACQUIRES, COLLECTS, AND STORES PLAINTIFF'S AND CLASS MEMBERS' PII

44. MCG has historically acquired, collected, and stored the PII of Plaintiff and Class Members.

45. Plaintiff and Class Members' sensitive and confidential PII is provided to MCG by their medical providers. MCG retains this information.

46. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

47. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on MCG to keep their PII confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

48. MCG could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiff and Class Members.

---

[3] *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 June 17, 2022).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

49. MCG's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

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

MCG KNEW OR SHOULD HAVE KNOWN THE RISK BECAUSE THE MEDICAL SERVICES SECTOR IS PARTICUALRY SUSCEPTIBLE TO CYBERATTACKS

51. Defendant knew and understood unprotected or exposed PII in the custody of companies operating in the health care industry, such as Defendant, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that PII through unauthorized access.

Value of Personally Identifiable Information

52. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[4] 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."[5]

53. 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, PII can be sold at a price ranging from $40 to $200, and bank

[4] 17 C.F.R. § 248.201 (2013).
[5] *Id*.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

details have a price range of $50 to $200.[6] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[7] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[8]

54. Social Security numbers, for example, are among the worst kind of PII 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:

> 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.[9]

55. 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.

---

[6] *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 June 17, 2022).

[7] *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 June 17, 2022).

[8] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited June 17, 2022).

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

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

56. 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."[10]

57. 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 compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number, driver's license number, name, and date of birth.

58. 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."[11]

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

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

---

[10] 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 June 17, 2022).

[11] 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 June 17, 2022).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

61. 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 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.[12]

62. 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, 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.

63. 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.

64. 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.

65. In the breach notification letter, Defendant made an offer of 12 months of identity monitoring services. This is wholly inadequate to compensate Plaintiff and Class Members as it

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

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, and medical and financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII.

66. 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.

67. 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, fraudulent use of that information and damage to victims may continue for years.

Defendant failed to properly protect Plaintiff's and Class Members' PII

68. Defendant breached its obligations to Plaintiff and Class Members and was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems 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, cyber-attacks, hacking incidents, and ransomware attacks;

b. Failing to adequately protect patients' PII;

c. Failing to properly monitor its own data security systems for existing or prior intrusions;

d. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

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

f. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

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

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

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

j. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

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

l. Failing to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR § 164.304's definition of "encryption");

m. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act, and;

n. Failing to adhere to industry standards for cybersecurity.

69. As the result of computer systems in need of security upgrades, inadequate procedures for handling email phishing attacks, viruses, malignant computer code, hacking attacks, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII.

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

Cyberattacks and data breaches cause disruption and put individuals at an increased risk of fraud and identity theft

71. Hacking incidents and data breaches at healthcare related companies like Defendant are especially problematic because of the sensitive nature of the information at issue and the disruption they cause to the medical treatment and overall daily lives of patients affected by the attack.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

72. Researchers have found that at medical facilities that experienced a data security incident, the death rate among patients increased in the months and years after the attack.[13]

73. Researchers have further found that at medical facilities that experienced a data security incident, the incident was associated with deterioration in timeliness and patient outcomes, generally.[14]

74. 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]

75. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a

---

[13] *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks.

[14] *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.

[15] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007). Available at https://www.gao.gov/new.items/d07737.pdf.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

victim's identity, such as a person's login credentials or Social Security number. 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.

76. 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 7 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]

77. 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.

78. Identity thieves can also use Social Security numbers 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. 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.

[16] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited June 17, 2022).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

79. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent

PLAINTIFF'S AND CLASS MEMBERS' DAMAGES

80. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences if its data security, or agent's data security systems were breached, including the significant costs that would be imposed on Plaintiff and the Class as a result of the breach.

81. As a direct and proximate result of Defendant's conduct, Plaintiff and the other Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

82. As a result of the Breach, Plaintiff and the other Class Members must now be vigilant and review their credit reports for suspected incidents of identity theft, and educate themselves about security freezes, fraud alerts, and other steps to protect themselves against identity theft. The need for additional monitoring for identity theft and fraud will extend indefinitely into the future.

83. Even absent any adverse use, consumers suffer injury from the simple fact that information associated with their financial accounts and identity has been stolen. When such sensitive information is stolen, accounts become less secure and the information once used to sign up for bank accounts and other financial services is no longer as reliable as it had been before the theft. Thus, consumers must spend time and money to re-secure their financial position and rebuild the good standing they once had in the financial community.

84. Plaintiff and the other Class Members have suffered and will suffer actual injury

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

due to loss of time and increased risk of identity theft as a direct result of the Breach. In addition to fraudulent charges, loss of use of and access to their account funds, costs associated with their inability to obtain money from their accounts, diminution of value of the data, and damage to their credit, Plaintiff and the other Class Members suffer ascertainable losses in the form of out-of-pocket expenses, opportunity costs, and the time and costs reasonably incurred to remedy or mitigate the effects of the Breach, including:

a. Monitoring compromised accounts for fraudulent charges;

b. Canceling and reissuing credit and debit cards linked to the financial information in possession of Defendant;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Taking trips to banks and waiting in line to verify their identities in order to restore access to the accounts;

g. Placing freezes and alerts with credit reporting agencies;

h. Spending time on the phone with or at financial institutions to dispute fraudulent charges;

i. Contacting their financial institutions and closing or modifying financial accounts;

j. Resetting automatic billing and payment instructions from compromised credit and debit cards to new cards;

k. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised accounts that had to be cancelled; and,

l. Closely reviewing and monitoring financial accounts and credit reports for unauthorized activity for years to come.

85. Moreover, Plaintiff and the other Class Members have an interest in ensuring that

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Defendant implement reasonable security measures and safeguards to maintain the integrity and confidentiality of the PII, including making sure that the storage of data or documents containing PII is not accessible by unauthorized persons and that access to such data is sufficiently protected.

86. And finally, as a direct and proximate result of Defendant's actions and inactions, Plaintiff and the other Class Members have suffered out-of-pocket losses, anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

87. In addition to the remedy for economic harm, Plaintiff and the Class Members maintain an undeniable and continuing interest in ensuring that the PII remains in the possession of Defendant is secure, remains secure, and is not subject to future theft.

Plaintiff Cynthia Strecker's Experience

88. Plaintiff typically takes measures to protect her PII and is very careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or other unsecured source.

89. Plaintiff stores any documents containing her PII in a safe and secure location. She also diligently chooses unique usernames and passwords for her online accounts.

90. As a result of the Data Breach, Plaintiff has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach. She monitors accounts and credit scores and has sustained emotional distress as a result of worrying about her PII being exfiltrated. She has monitored her Credit Karma account extensively since receiving the Notice of Data Incident from Defendant, and intends to spend time taking steps to

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

protect her PII. This is time that was and will be lost and unproductive and taken away from other activities and duties.

91. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety, emotional distress, and increased concerns for the loss of her privacy.

92. As a result of the Data Breach and the exfiltration of her unencrypted PII in the hands of criminals, Plaintiff is at a substantial present risk and will continue to be at an increased risk of identity theft and fraud for years to come.

93. To date, Defendant has done very little to adequately protect Plaintiff and Class Members, or to compensate them for their injuries sustained in this Data Breach. It offered identity monitoring services, but only for two years, which is wholly inadequate for a data breach including Plaintiff's and Class Members' Social Security numbers.

CLASS ALLEGATIONS

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

> **All persons MCG identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach.**

95. Excluded from the Classes 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; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

96. **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. The identities of Class Members are ascertainable through MCG's records, Class Members' records, publication notice, self-identification, and other means.

97. **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 MCG unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

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

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

d. Whether MCG's data security systems before and during the Data Breach were consistent with industry standards;

e. Whether MCG owed a duty to Class Members to safeguard their PII;

f. Whether MCG breached its duty to Class Members to safeguard their PII;

g. Whether computer hackers obtained Class Members' PII in the Data Breach;

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

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of MCG's misconduct;

j. Whether MCG's conduct was negligent;

k. Whether MCG violated consumer protection laws, and,

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

l. Whether Plaintiff and Class Members are entitled to damages, civil penalties, and/or injunctive relief.

98. **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.

99. **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.

100. **Predominance.** MCG 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.

101. **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 MCG. 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.

102. MCG 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

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Class-wide basis.

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

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

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

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

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

104. Finally, all members of the proposed Class are readily ascertainable. MCG 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 MCG.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

105. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 104.

106. MCG knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' PII, and had a duty to exercise reasonable care in safeguarding, securing,

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

107. MCG 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' PII.

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

109. 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' 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.

110. MCG 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.

111. MCG had a duty to employ reasonable security measures and otherwise protect the PII of Plaintiff and Class Members.

112. MCG, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' PII within MCG's possession.

113. MCG, 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' PII.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

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

115. MCG's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' PII to be compromised.

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

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

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

119. Plaintiff seeks the award of actual damages on behalf of herself and the Class.

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

SECOND CAUSE OF ACTION
Violation of the Washington State Consumer Protection Act
(RCW 19.86.010 *et seq*.)
(On Behalf of Plaintiff and the Nationwide Class)

121. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 120.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

122. The Washington State Consumer Protection Act, RCW 19.86.020 (the "CPA") prohibits any "unfair or deceptive acts or practices" in the conduct of any trade or commerce as those terms are described by the CPA and relevant case law.

123. Defendant is a "person" as described in RWC 19.86.010(1).

124. Defendant engages in "trade" and "commerce" as described in RWC 19.86.010(2) in that they engage in the sale of services and commerce directly and indirectly affecting the people of the State of Washington.

125. Defendant is headquartered in Washington; its strategies, decision-making, and commercial transactions originate in Washington; most of its key operations and employees reside, work, and make company decisions (including data security decisions) in Washington; and Defendant and many of its employees are part of the people of the State of Washington.

126. In the course of conducting their business, Defendant committed "unfair acts or practices" by, inter alia, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members' PII. Plaintiff and Class Members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. As described above, Defendant's unfair acts and practices ongoing and continue to this date.

127. Defendant's conduct was also deceptive. Defendant failed to timely notify and concealing from Plaintiff and Class Members the unauthorized release and disclosure of their PII. If Plaintiff and Class Members had been notified in an appropriate fashion, and had the

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

information not been hidden from them, they could have taken precautions to safeguard and protect their PII, medical information, and identities.

128. Defendant's above-described "unfair or deceptive acts or practices" in violation effects the public interest because it is substantially injurious to persons, had the capacity to injure other persons, and has the capacity to injure other persons.

129. The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

130. Defendant's above-described unfair and deceptive acts and practices directly and proximately caused injury to Plaintiff and Class Members' business and property. Plaintiff and Class Members have suffered, and will continue to suffer, actual damages and injury in the form of, inter alia, (1) an imminent, immediate and the continuing increased risk of identity theft, identity fraud and medical fraud—risks justifying expenditures for protective and remedial services for which he or she is entitled to compensation; (2) invasion of privacy; (3) breach of the confidentiality his or her PII; (5) deprivation of the value of his or her PII, for which there is a well-established national and international market; (6) the financial and temporal cost of monitoring credit, monitoring financial accounts, and mitigating damages; and/or (7) investment of substantial time and money to monitoring and remediating the harm inflicted upon them

131. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiff, therefore, on behalf of herself, Class Members, and the general public, also seeks restitution and an injunction prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

modify their corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII entrusted to it.

132. Plaintiff, on behalf of Plaintiff and the Class Members, also seeks to recover actual damages sustained by each class member together with the costs of the suit, including reasonable attorney fees. In addition, Plaintiff, on behalf of Plaintiff and the Class Members, requests that this Court use its discretion, pursuant to RCW 19.86.090, to increase the damages award for each class member by three times the actual damages sustained not to exceed $25,000.00 per class member.

PRAYER FOR RELIEF

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

A. For an order certifying the Class, as defined herein, and appointing Plaintiff and her Counsel to represent each such 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 PII of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to 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

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

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 PII of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the 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;

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

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 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

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

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 PII 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, statutory, nominal, and consequential 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.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

DEMAND FOR JURY TRIAL

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

Dated: June 20, 2022

TOUSLEY BRAIN STEPHENS PLLC

By: *s/ Jason T. Dennett*
Jason T. Dennett, WSBA #30686
s/ Rebecca L. Solomon
Rebecca L. Solomon, WSBA #51520
1200 Fifth Avenue, Suite 1700
Seattle, WA 98101-3147
Tel: (206) 682-5600/Fax: (206) 682-2992
jdennett@tousley.com
rsolomon@tousley.com

Terence R. Coates (*pro hac vice* forthcoming)
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com

Joseph M. Lyon (*pro hac vice* forthcoming)
THE LYON FIRM
2754 Erie Avenue
Cincinnati, OH 45208
Phone: (513) 381-2333
Fax: (513) 721-1178
jlyon@thelyonfirm.com

Counsel for Plaintiff and Putative Class Members

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: MCG Health Hit with Class Action Over March 2022 Data Breach Affecting 1.1M Patients