UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND

In re Retina Group of Washington Data Security Incident Litigation	Lead Case No.: 8:24-cv-00004-TDC **CONSOLIDATED CLASS ACTION COMPLAINT** **JURY DEMAND**

Plaintiffs Mary Vandenbroucke, Katherine Traynham, Kwame Dapaah-Siakwan, Jennifer Boehles, Shalane Vance, Sharon Jenkins, Natalia Girard, David Puckett, and Desiree McCormick ("Plaintiffs") bring this Consolidated Class Action Complaint ("Complaint") against Defendant The Retina Group of Washington, PLLC ("Defendant" or "RGW") as individuals and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiffs bring this Complaint against RGW for its failure to properly secure and safeguard the sensitive information that it collected and maintained as part of its regular business practices, including names, dates of birth, driver's license numbers or other government-issued identification numbers, addresses, telephone numbers, demographic information, payment information, Social Security numbers ("personally identifying information" or "PII") and medical and health insurance information, which is protected health information ("PHI", and collectively with PII, "Private Information") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

2. Plaintiffs bring this action on behalf of all persons whose Private Information was compromised as a result of RGW's failure to: (i) adequately protect the Private Information of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of RGW's inadequate

information security practices; and (iii) effectively secure hardware containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents. RGW's conduct amounts at least to negligence and violates federal and state statutes.

3. As a result of RGW's misconduct, Plaintiffs and Class Members have sustained actual injuries and damages, as alleged below.

4. Plaintiffs 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 who remain at risk due to RGW's inadequate data security practices.

PARTIES

5. Plaintiff Mary Vandenbroucke is a resident and citizen of Maryland.

6. Plaintiff Katherine Traynham is a resident and citizen of Virginia.

7. Plaintiff Kwame Dapaah-Siakwan is a resident and citizen of Virginia.

8. Plaintiff Jennifer Boehles is a resident and citizen of Maryland.

9. Plaintiff Shalane Vance is a resident and citizen of Maryland.

10. Plaintiff Sharon Jenkins is a resident and citizen of Washington, D.C.

11. Plaintiff Natalia Girard is a resident and citizen of Maryland.

12. Plaintiff David Puckett is a resident and citizen of Virginia.

13. Plaintiff Desiree McCormick is a resident and citizen of Maryland.

14. Defendant The Retina Group of Washington, PLLC is a Virginia limited liability company, with its principal place of business located in Greenbelt, Maryland.

JURISDICTION AND VENUE

15. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because at least one member of the putative Class, as defined below, is a citizen of a different state than RGW,[1] there are more than 100 putative class members, and the amount in controversy exceeds $5 million exclusive of interest and costs.

16. This Court has general personal jurisdiction over RGW because it maintains its principal place of business in this District.

17. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because RGW's principal place of business is in this District.

STATEMENT OF FACTS

RGW's Business

18. RGW is a healthcare company that provides medical services to its patients, including "specialized ophthalmology for retina diseases and vitreoretinal surgery" and "procedures in treating retinal diseases, conditions and disorders."[2]

19. In order to obtain medical services from RGW, RGW requires its patients to provide sensitive and confidential Private Information, including, but not limited to, their names, dates of birth, and Social Security numbers.

20. RGW retains and stores this information and derives a substantial economic benefit from the Private Information that it collects. But for the collection of Plaintiffs' and Class Members' Private Information, RGW would be unable to perform its services.

[1] According to the report submitted to the commonwealth of Massachusetts, 464 Massachusetts residents were impacted in the Data Breach. *See* https://www.mass.gov/doc/data-breach-report-2023/download.

[2] *Homepage*, Retina Grp. of Wash., https://www.rgw.com/ (last accessed Mar. 13, 2024).

21. The information held by RGW in its computer systems included the unencrypted Private Information of Plaintiffs and Class Members.

22. By obtaining, collecting, and storing the Private Information of Plaintiffs and Class Members, RGW assumed legal and equitable duties and knew or should have known that they were responsible for protecting the Private Information from disclosure.

23. Upon information and belief, RGW made promises and representations to its patients that the Private Information collected from them as a condition of obtaining medical services at RGW would be kept safe, confidential, that the privacy of that information would be maintained, and that RGW would delete any sensitive information after it was no longer required to maintain it.

24. Indeed, RGW provides on its website that: "[w]e are required by law to: [] make sure that medical information that identifies you is kept private[.]"[3]

25. Furthermore, upon information and belief, RGW provides every patient with a HIPAA compliant disclosure form in which it represents that it will protect patients' Private Information.

26. Plaintiffs and Class Members provided their Private Information to RGW with the reasonable expectation and mutual understanding that RGW would comply with its obligations to keep such information confidential and secure from unauthorized access.

27. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiffs and Class Members relied on the sophistication of RGW to keep their Private Information confidential and securely maintained, to

[3] *Notice of Privacy Practices*, PRISM Vision Grp. (Feb. 21, 2022), https://prismvisiongroup.com/wordpress/wp-content/uploads/2022/02/PRISM-Notice-of-Privacy-Practices-Revised-2.21.22.pdf.

use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

The Data Breach

28. On or about December 22, 2023, RGW began sending Plaintiffs and other victims of the Data Breach an untitled letter (the "Notice Letter"). The Notice Letter informed Class members that RGW experienced a data breach on March 26, 2023, which exposed Class members' Personal Information, including a Class Member's "name, Social Security number, driver's license number or other government-issued identification number, medical record number, address, telephone number, email address, date of birth, date of service, and/or other demographic information as well as health, payment, and/or insurance information." [4]

29. RGW did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiffs and Class Members, such as encrypting the information or deleting it when it is no longer needed. These failings ultimately caused the exposure of Private Information in the Data Breach.

30. The attacker accessed and acquired files in RGW's computer systems containing unencrypted Private Information of Plaintiffs and Class Members, including but not limited to their names, dates of birth, PHI, and Social Security numbers.

Data Breaches are Preventable

[4] The "Notice Letter". A sample copy is available at https://www.rgw.com/wp-content/uploads/2023/07/FINAL-6.30.23-RGW-Website-Notice.pdf.

31. To prevent and detect cyber-attacks and/or ransomware attacks, RGW 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.
- 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.[5]

32. Given that RGW was storing the sensitive Private Information of its current and former patients, RGW could and should have implemented all of the above measures to prevent and detect cyberattacks.

33. The occurrence of the Data Breach indicates that RGW failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach

[5] *See* How to Protect Your Networks from RANSOMWARE, at 3, available at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Aug. 23, 2021).

and the exposure of the Private Information of more than four hundred thousand individuals,[6] including that of Plaintiffs and Class Members.

RGW Knew, or Should Have Known, of the Risk Because Healthcare Entities in Possession of Private Information are Particularly Susceptible to Cyber Attacks

34. Data thieves regularly target companies like RGW's due to the highly sensitive information that they custody. In the third quarter of the 2023 fiscal year alone, 7333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.[7]

35. As a custodian of Private Information, RGW knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiffs and Class Members, and of the foreseeable consequences if its data security systems were breached.

36. RGW was, or should have been, fully aware of the unique type and the significant volume of data on RGW's server(s), amounting to more than four hundred thousand individuals' detailed Private Information, and thus the significant number of individuals who would be harmed by the exposure of the unencrypted data.

37. The injuries to Plaintiffs and Class Members were directly and proximately caused by RGW's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

---

[6] *Cases Currently Under Investigation*, U.S. Dep't of Health & Human Servs., https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Mar. 13, 2024).

[7] *See ITRC Q3 Data Breach Analysis*, Identity Theft Res. Ctr., https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/ (last accessed Mar. 13, 2024).

Value of Private Information

38. 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.[8]

39. For example, Personal Information can be sold at a price ranging from $40 to $200.[9] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[10]

40. Driver's license numbers, which were compromised in the Data Breach, are incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information."[11] 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.[12]

41. Theft of PHI is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[13]

---

[8] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

[9] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

[10] *In the Dark*, VPNOverview (2019), https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.

[11] *Hackers Stole Customers' License Numbers From Geico In Months-Long Breach*, Forbes (Apr. 20, 2021), https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3bda585e8658.

[12] *Id.*

[13] *Medical I.D. Theft*, EFraudPrevention, https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected (last accessed Mar. 13, 2024).

42. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—names, dates of birth, PHI, and Social Security numbers.

43. 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 . . . [is] worth more than 10x on the black market."[14]

44. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. Plaintiffs 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 Private Information.

RGW Fails to Comply with FTC Guidelines

45. 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.

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

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

understand their network's vulnerabilities; and implement policies to correct any security problems.[15]

47. 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.[16]

48. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential patient 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.

49. These FTC enforcement actions include actions against healthcare entities, like RGW. *See, e.g.*, *In the Matter of LabMD, Inc., a corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

50. RGW failed to properly implement basic data security practices. RGW's failure to employ reasonable and appropriate measures to protect against unauthorized access to its patients'

[15] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.
[16] *Id.*

Private Information or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

RGW Fails to Comply With HIPAA Guidelines

51. RGW is a covered entity under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

52. RGW is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[17] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

53. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

54. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

55. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

[17] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

56. "Electronic protected health information" is "individually identifiable health information . . . that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

57. HIPAA's Security Rule requires RGW to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

58. HIPAA also requires RGW to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, RGW is required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

59. HIPAA and HITECH also obligated RGW to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1), (3); *see also* 42 U.S.C. § 17902.

60. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400–164.414, also requires RGW to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."[18]

61. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

62. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

63. HIPAA also requires the Office of Civil Rights ("OCR") within the Department of Health and Human Services ("HHS") to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302–164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule."[19] The list of resources includes a link to guidelines set by the National

[18] *Breach Notification Rule*, U.S. Dep't of Health & Human Servs., https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last accessed Mar. 13, 2024).

[19] *Security Rule Guidance Material*, U.S. Dep't of Health & Human Servs., http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last accessed Mar. 13, 2024).

Institute of Standards and Technology ("NIST"), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI."[20]

RGW Fails to Comply with Industry Standards

64. Several best practices have been identified that, at a minimum, should be implemented by healthcare entities in possession of Private Information, like RGW, 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. RGW failed to follow these industry best practices, including a failure to implement multi-factor authentication.

65. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protection against any possible communication system; and training staff regarding critical points. RGW failed to follow these cybersecurity best practices, including failure to train staff.

66. RGW 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.

[20] *Guidance on Risk Analysis*, U.S. Dep't of Health & Human Servs., https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html (last accessed Mar. 13, 2024).

67. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and upon information and belief, RGW failed to comply with at least one—or all—of these accepted standards, thereby permitting and causing the Data Breach to occur.

The Data Breach Increases Plaintiffs' and Class Members' Risk of Identity Theft

68. The unencrypted Private Information of Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers.

69. Plaintiffs' and Class Members' Private Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiffs and Class Members and to profit off their misfortune.

70. For example, with "Fullz packages"[21] cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

71. The development of "Fullz" packages means that the stolen Private Information can

[21] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Sec. (Sep. 18, 2014), https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm/.

easily be used to link and identify Plaintiffs' and Class Members' sensitive information.

Loss of Time to Mitigate the Risk of Identity Theft and Fraud

72. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching the Data Breach to verify the incident and obtain more details on its occurrence, changing passwords and resecuring their own computer networks, and contacting financial institutions to sort out fraudulent activity on their accounts.

73. Plaintiffs' mitigation efforts are consistent with the steps that FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[22]

Diminution of Value of Private Information

74. PII and PHI are valuable property rights. Their value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include significant penalties.

75. Sensitive PII can sell for as much as $363 per record according to the Infosec Institute.[23] An active and robust legitimate marketplace for PII also exists. In 2019, the data

[22] *See Steps*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last accessed Mar. 13, 2024).

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

brokering industry was worth roughly $200 billion.[24]

76. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss.

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

77. Given the type of targeted attack in this case, sophisticated criminal activity, and the type of Private Information involved, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for fraud.

78. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that their Private Information was used to file for unemployment benefits until law enforcement notifies their employer of the suspected fraud. Fraudulent tax returns are typically discovered when an authentic tax return is rejected.

Loss of Benefit of the Bargain

79. Furthermore, RGW's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to obtain services at RGW under certain terms, Plaintiffs and other reasonable patients understood and expected that RGW would properly safeguard and protect their Private Information, when in fact, RGW did not provide the expected data security. Accordingly, Plaintiffs and Class Members received medical services of a lesser value than what they reasonably expected to receive under the bargains they struck with RGW.

[24] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

PLAINTIFFS' AND CLASS MEMBERS' COMMON INJURIES

80. As a result of RGW's ineffective and inadequate data security practices, the Data Breach occurred, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent. Plaintiffs and Class Members have all sustained injuries and damages, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of their Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in RGW's possession and is subject to further unauthorized disclosures so long as RGW fails to undertake appropriate and adequate measures to protect the Private Information.

81. Moreover, due to the actual and imminent risk of identity theft that Plaintiffs and Class Members face, RGW in its Notice Letter., instructs recipients to take the following measures to protect themselves: "remain vigilant against incidents of identity theft and fraud, to review their account and explanation of benefits statements, and to monitor their free credit reports for suspicious activity and to detect errors."[25]

82. Additionally, the Data Breach has caused Plaintiffs and Class Members to suffer fear, anxiety, and stress, which has been compounded by the fact that RGW has still not fully informed them of key details about the Data Breach's occurrence.

[25] Notice Letter.

83. Plaintiffs and Class Members have a continuing interest in ensuring their Private Information, which, upon information and belief, remains backed up in RGW's possession, is protected and safeguarded from future breaches.

PLAINTIFFS' EXPERIENCES

Plaintiff Mary Vandenbroucke

84. Plaintiff Vandenbroucke obtained services at RGW as a patient in the past. As a condition of obtaining services, she was required to provide RGW with her Private Information.

85. Upon information and belief, at the time of the Data Breach, RGW retained Plaintiff Vandenbroucke's Private Information in its system.

86. Plaintiff Vandenbroucke is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

87. Plaintiff Vandenbroucke received the Notice Letter, by U.S. mail, directly from RGW, in or about December 2023, informing her that her Private Information was improperly accessed and obtained by unauthorized third parties during the Data Breach.

88. As a result of the Data Breach and at the direction of the Notice Letter, Plaintiff Vandenbroucke made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching and verifying the legitimacy of the Data Breach.

Plaintiff Katherine Traynham

89. Plaintiff Traynham obtained services at RGW as a patient in the past. As a condition of obtaining services, she was required to provide RGW with her Private Information.

90. Upon information and belief, at the time of the Data Breach, RGW retained Plaintiff Traynham's Private Information in its system.

91. Plaintiff Traynham is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

92. Plaintiff Traynham received the Notice Letter, by U.S. mail, directly from RGW, in or about December 2023, informing her that her Private Information was improperly accessed and obtained by unauthorized third parties during the Data Breach.

93. As a result of the Data Breach and at the direction of the Notice Letter, Plaintiff Traynham made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching and verifying the legitimacy of the Data Breach.

94. Plaintiff Traynham has spent approximately 22 hours to date taking action to attempt to prevent or mitigate additional harms from the Data Breach, including checking her financial accounts for signs of fraud, monitoring her health portals and medical information for misuse, and monitoring her credit. Additionally, she spent time contacting her credit card companies to inform them of the Data Breach and signing up for credit monitoring protection.

Plaintiff Kwame Dapaah-Siakwan

95. Plaintiff Dapaah-Siakwan obtained services at RGW as a patient in or about 2023. As a condition of obtaining services, he was required to provide RGW with his Private Information.

96. Upon information and belief, at the time of the Data Breach, RGW retained Plaintiff Dapaah-Siakwan's Private Information in its system.

97. Plaintiff Dapaah-Siakwan is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

98. Plaintiff Dapaah-Siakwan received the Notice Letter, by U.S. mail, directly from RGW, in or about December 2023, informing him that his Private Information was improperly accessed and obtained by unauthorized third parties during the Data Breach.

99. As a result of the Data Breach and at the direction of the Notice Letter, Plaintiff Dapaah-Siakwan made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach to verify the incident and obtain more details on its occurrence, changing passwords and resecuring his own computer network, contacting financial institutions to sort out fraudulent activity on their accounts, and replacing impacted debit cards.

100. Plaintiff Dapaah-Siakwan also suffered injury in the form of experiencing fraudulent charges, for approximately $20, to his Wells Fargo debit card, in or about November 2023, which, upon information and belief, was caused by the Data Breach.

101. Plaintiff Dapaah-Siakwan further suffered injury in the form of his credit score being damaged, which, upon information and belief, was caused by the Data Breach.

102. Plaintiff Dapaah-Siakwan further suffered injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

Plaintiff Jennifer Boehles

103. Plaintiff Boehles obtained services at RGW as a patient in the past. As a condition of obtaining services, she was required to provide RGW with her Private Information.

104. Upon information and belief, at the time of the Data Breach, RGW retained Plaintiff Boehles's Private Information in its system.

105. Plaintiff Boehles is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

106. Plaintiff Boehles received the Notice Letter, by U.S. mail, directly from RGW, in or about December 2023, informing her that her Private Information was improperly accessed and obtained by unauthorized third parties during the Data Breach.

107. Soon after the Data Breach, Plaintiff Boehles received notices from several financial institutions with which she has accounts, including Chase Bank, Discover, and Bank of America, that her account information may have been tampered with and/or otherwise compromised.

108. Plaintiff Boehles also received multiple targeted phishing emails attempting to further misuse her Private Information.

109. As a result of the Data Breach and at the direction of the Notice Letter, Plaintiff Boehles made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: reviewing financial accounts for any indications of actual or attempted identity theft or fraud, updating her financial account information, activating new debit and credit cards, and researching the credit monitoring offered by RGW.

Plaintiff Shalane Vance

110. Plaintiff Shalane Vance obtained services at RGW as a patient in or about 2021. As a condition of obtaining services, she was required to provide RGW with her Private Information.

111. Upon information and belief, at the time of the Data Breach, RGW retained Plaintiff Vance's Private Information in its system.

112. Plaintiff Vance is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

113. Plaintiff Vance received the Notice Letter, by U.S. mail, directly from RGW, in or about December 2023, informing her that her Private Information was improperly accessed and obtained by unauthorized third parties during the Data Breach.

114. As a result of the Data Breach and at the direction of the Notice Letter, Plaintiff Vance made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud.

115. Plaintiff Vance further suffered injury in the form of her credit score being damaged, which, upon information and belief, was caused by the Data Breach.

116. Plaintiff Vance further suffered injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

Plaintiff Sharon Jenkins

117. Plaintiff Jenkins is a current patient at RGW. As a condition of obtaining services, she was required to provide RGW with her Private Information.

118. Upon information and belief, at the time of the Data Breach, RGW retained Plaintiff Jenkins's Private Information in its system.

119. Plaintiff Jenkins is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

120. Plaintiff Jenkins received the Notice Letter, by U.S. mail, directly from RGW, in or about December 2023, informing her that her Private Information was improperly accessed and obtained by unauthorized third parties during the Data Breach.

121. As a result of the Data Breach and at the direction of the Notice Letter, Plaintiff Jenkins made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud.

122. Plaintiff Jenkins further suffered injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

Plaintiff Natalia Girard

123. Plaintiff Girard obtained services at RGW as a patient in the past. As a condition of obtaining services, she was required to provide RGW with her Private Information.

124. Upon information and belief, at the time of the Data Breach, RGW retained Plaintiff Girard's Private Information in its system.

125. Plaintiff Girard is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

126. Plaintiff Girard received the Notice Letter, by U.S. mail, directly from RGW, in or about December 2023, informing her that her Private Information was improperly accessed and obtained by unauthorized third parties during the Data Breach.

127. As a result of the Data Breach and at the direction of the Notice Letter, Plaintiff Girard made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: time spent verifying the legitimacy and impact of the Data Breach; time spent exploring credit monitoring and identity theft insurance options; time spent self-monitoring their accounts with heightened scrutiny; and time spent seeking legal counsel regarding their options for remedying and/or mitigating the effects of the Data Breach.

128. Plaintiff Girard further suffered injury in the form of her Private Information being disseminated on the dark web, according to CreditWise, which, upon information and belief, was caused by the Data Breach.

Plaintiff David Puckett

129. Plaintiff Puckett is a current patient at RGW. As a condition of obtaining services, he was required to provide RGW with his Private Information.

130. Upon information and belief, at the time of the Data Breach, RGW retained Plaintiff Puckett's Private Information in its system.

131. Plaintiff Puckett is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

132. Plaintiff Puckett received the Notice Letter, by U.S. mail, directly from RGW, in or about December 2023, informing him that his Private Information was improperly accessed and obtained by unauthorized third parties during the Data Breach.

133. As a result of the Data Breach and at the direction of the Notice Letter, Plaintiff Puckett made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach, reviewing financial statements, monitoring his credit information, replacing his banking cards, and communicating with his bank about the fraudulent charges he experienced.

134. Plaintiff Puckett further suffered injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

Plaintiff Desiree McCormick

135. Plaintiff McCormick is a current patient at RGW. As a condition of obtaining services, she was required to provide RGW with her Private Information.

136. Upon information and belief, at the time of the Data Breach, RGW retained Plaintiff McCormick's Private Information in its system.

137. Plaintiff McCormick is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

138. Plaintiff McCormick received the Notice Letter, by U.S. mail, directly from RGW, in or about December 2023, informing her that her Private Information was improperly accessed and obtained by unauthorized third parties during the Data Breach.

139. As a result of the Data Breach and at the direction of the Notice Letter, Plaintiff McCormick made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: time spent verifying the legitimacy and impact of the Data Breach; time spent exploring credit monitoring and identity theft insurance options; time spent self-monitoring their accounts with heightened scrutiny and time spent seeking legal counsel regarding their options for remedying and/or mitigating the effects of the Data Breach.

140. Plaintiff McCormick further suffered injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

CLASS ACTION ALLEGATIONS

141. Pursuant to Federal Rule of Civil Procedure 23, Plaintiffs propose the following Class definitions, subject to amendment as appropriate:

> **Nationwide Class**
> All persons in the United States whose Private Information was maintained on RGW's computer systems that were compromised in the Data Breach announced by RGW in December 2023 (the "Class").
>
> **Maryland Subclass**
> All persons in the state of Maryland whose Private Information was maintained on RGW's computer systems that were compromised in the Data Breach announced by RGW in December 2023 (the "Maryland Subclass").[26]

142. Excluded from the Classes are RGW's officers and directors, and any entity in which RGW has a controlling interest; the affiliates, legal representatives, attorneys, successors, heirs, and assigns of RGW; and members of the judiciary to whom this case is assigned, their families, and members of their staff.

[26] For the avoidance of doubt, all Maryland Subclass members are also members of the Nationwide Class.

143. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. According to the report submitted to the U.S. Department of Health and Human Services, at least 455,000 individuals were impacted in the Data Breach.[27]

144. 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 RGW unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

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

d. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

e. Whether RGW was unjustly enriched by retention of the monetary benefits conferred on it by Plaintiffs and Class Members; and

f. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

145. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach.

146. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions.

[27] *Cases Currently Under Investigation*, *supra* note 6.

147. Predominance. RGW has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' Private Information was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from RGW's conduct affecting Class Members set out above predominate over any individualized issues.

148. 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.

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

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

150. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

151. RGW knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, 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.

152. RGW had, and continues to have, a duty to timely disclose that Plaintiffs' and Class Members' Private Information within its possession was compromised and precisely the type(s) of information that were compromised.

153. RGW, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within RGW's possession and by failing to timely disclose to Plaintiffs and Class Members that their Private Information within RGW's possession might have been compromised and precisely the type of information compromised.

154. As a direct and proximate result of RGW's negligence, Plaintiffs and Class Members suffered injuries, as alleged herein.

155. In failing to secure Plaintiffs' and Class Members' Private Information and promptly notifying them of the Data Breach, RGW is guilty of oppression, fraud, or malice, in that RGW acted or failed to act with a willful and conscious disregard of Plaintiffs' and Class Members' rights.

156. Plaintiffs seek injunctive relief on behalf of the Class in the form of an order (1) compelling RGW to institute appropriate data collection and safeguarding methods and policies with regard to patient information; and (2) compelling RGW to provide detailed and specific disclosure of what types of Private Information have been compromised as a result of the data breach.

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

157. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

158. Plaintiffs and the Class entrusted their Private Information to RGW. In so doing, Plaintiffs and the Class entered into implied contracts with RGW by which RGW agreed to safeguard and protect such information, to keep such information secure and confidential, and

to timely and accurately notify Plaintiffs and the Class if their data had been breached and compromised or stolen.

159. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that RGW's data security practices complied with relevant laws and regulations and were consistent with industry standards.

160. Implicit in the agreement between Plaintiffs and Class Members and the RGW to provide Private Information, was the latter's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiffs and Class Members from unauthorized disclosure or uses, (f) retain the Private Information only under conditions that kept such information secure and confidential.

161. The mutual understanding and intent of Plaintiffs and Class Members on the one hand, and RGW, on the other, is demonstrated by their conduct and course of dealing.

162. RGW solicited, offered, and invited Plaintiffs and Class Members to provide their Private Information as part of RGW's regular business practices. Plaintiffs and Class Members accepted RGW's offers and provided their Private Information to RGW.

163. In accepting the Private Information of Plaintiffs and Class Members, RGW understood and agreed that it was required to reasonably safeguard the Private Information from unauthorized access or disclosure.

164. Plaintiffs and Class Members paid money and provided their Private Information to RGW with the reasonable belief and expectation that RGW would use part of its earnings to obtain adequate data security. RGW failed to do so.

165. Plaintiffs and Class Members would not have entrusted their Private Information to RGW in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

166. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with RGW.

167. RGW breached the implied contracts it made with Plaintiffs and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiffs and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

168. As a direct and proximate result of RGW's breach of the implied contracts, Plaintiffs and Class Members sustained damages, as alleged herein.

169. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach as well as injunctive relief requiring RGW to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT III
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

170. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

171. Plaintiffs and Class Members gave RGW their Private Information in confidence, believing that RGW would protect that information.

172. Plaintiffs and Class Members would not have provided RGW with this information had they known it would not be adequately protected. RGW's acceptance and storage of Plaintiffs' and Class Members' Private Information created a fiduciary relationship between RGW and Plaintiffs and Class Members.

173. In light of this relationship, RGW must act primarily for the benefit of its patients, which includes safeguarding and protecting Plaintiffs' and Class Members' Private Information.

174. Due to the nature of the relationship between RGW and Plaintiffs and Class Members, Plaintiffs and Class Members were entirely reliant upon RGW to ensure that their Private Information was adequately protected. Plaintiffs and Class Members had no way of verifying or influencing the nature and extent of RGW's data security policies and practices, and RGW was in an exclusive position to guard against the Data Breach.

175. RGW has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiffs' and Class Members' Private Information, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

176. As a direct and proximate result of RGW's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, as alleged herein.

COUNT IV
Intrusion Upon Seclusion
(By Plaintiffs and the Class)

177. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

178. Plaintiffs and Class Members had a reasonable expectation of privacy in the Private Information that RGW possessed and/or continues to possess.

179. By failing to keep Plaintiffs' and Class Members' Private Information safe, and by misusing and/or disclosing their Private Information to unauthorized parties for unauthorized use, RGW invaded Plaintiffs' and Class Members' privacy by: (a) intruding into their private affairs in a manner that would be highly offensive to a reasonable person; and (b) publicizing private facts about Plaintiffs and Class Members, which is highly offensive to a reasonable person.

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

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

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

183. In failing to protect Plaintiffs' and Class Members' Private Information, and in misusing and/or disclosing their Private Information, RGW has acted with malice and oppression and in conscious disregard of Plaintiffs' and Class Members rights to have such

information kept confidential and private, in failing to provide adequate notice, and in placing its own economic, corporate, and legal interests above the privacy interests of its thousands of patients. Plaintiffs, therefore, seek an award of damages, including punitive damages, on behalf of Plaintiffs and the Class.

COUNT V
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

184. Plaintiffs re-allege and incorporate the above allegations, as if fully set forth herein, and bring this claim in the alternative to the breach of implied contract and breach of fiduciary duty claims above.

185. Plaintiffs and Class Members conferred a monetary benefit on RGW. Specifically, they paid RGW for medical services from RGW as well as provided RGW with their Private Information. In exchange, Plaintiffs and Class Members should have received the medical services that were the subject of the transaction and had their Private Information protected with adequate data security.

186. RGW knew that Plaintiffs and Class Members conferred a benefit on it in the form their Private Information and/or payments made to or on their behalf as a necessary part of their receiving medical services at RGW. RGW appreciated and accepted that benefit. RGW profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes, including billing for its services.

187. Upon information and belief, RGW funds its data security measures entirely from its general revenue, including payments to or on behalf Plaintiffs and Class Members. As such, a portion of the payments made for the benefit of or on behalf of Plaintiffs and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to RGW.

188. RGW, however, failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not provide adequate data security in return for the benefit Plaintiffs and Class Members provided.

189. RGW would not be able to carry out an essential function of its regular business without the Private Information of Plaintiffs and Class Members and derived revenue by using it for business purposes. Plaintiffs and Class Members expected that RGW or anyone in RGW's position would use a portion of that revenue to fund adequate data security practices.

190. If Plaintiffs and Class Members knew that RGW had not reasonably secured their Private Information, they would not have allowed their Private Information to be provided to RGW or obtained medical services at RGW.

191. RGW enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, RGW instead calculated to increase its own profit at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of RGW's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

192. Under the principles of equity and good conscience, RGW should not be permitted to retain the money wrongfully obtained Plaintiffs and Class Members, because RGW failed to implement appropriate data management and security measures that are mandated by industry standards.

193. Plaintiffs and Class Members have no adequate remedy at law.

194. As a direct and proximate result of RGW's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, as alleged herein. RGW should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them. In the alternative, RGW should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for RGW's services.

COUNT VI
Violations of Maryland's Consumer Protection Act and the Maryland Personal Information Act
(On Behalf of Plaintiffs and the Class, or in the alternative, On Behalf of Plaintiffs Vandenbroucke, Boehles, Vance, Girard, McCormick the Maryland Subclass)

195. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein, and bring this claim pursuant to the Maryland Consumer Protection Act, § 13-101, *et seq.* and the Maryland Personal Information Protection Act, § 14-3501, *et seq.*

196. The purpose of the Maryland Consumer Protection Act is "to set certain minimum statewide standards for the protection of consumers across the State [of] [Maryland]." The Maryland Personal Information Protection Act was implemented to, among other things, "[t]o protect personal information from unauthorized access, use, modification, or disclosure . . . of an individual residing in the State [of] [Maryland]."

197. A violation of the Maryland Personal Information Protection Act "is an unfair or deceptive trade practice."

198. Independently, RGW has violated the Maryland Consumer Protection Act by engaging in the unfair and deceptive practices alleged herein. Pursuant to HIPAA (42 U.S.C. § 1302d *et seq.*), the FTCA, and Maryland law, RGW was required, but failed, to protect Plaintiffs' and the Class's Private Information and maintain adequate and reasonable data and

cybersecurity measures to maintain the security and privacy of Plaintiffs' and Class Members' Private Information. This constitutes a violation of Maryland's Consumer Protection Act.

199. The damages suffered by Plaintiffs and Class Members were directly and proximately caused by the deceptive, misleading, and unfair practices of RGW, as described above.

200. Plaintiffs and Class Members seek declaratory judgment that RGW's data security practices were not reasonable or adequate and caused the cyberattack under the Maryland CPA, as well as injunctive relief enjoining the above-described wrongful acts and practices of RGW and requiring RGW to employ and maintain industry accepted standards for data management and security.

PRAYER FOR RELIEF

WHEREFORE**,** Plaintiffs, on behalf of themselves and Class Members, request judgment against RGW and that the Court grants the following:

A. For an Order certifying this action as a class action and appointing Plaintiffs and their Counsel to represent the Classes;

B. For equitable relief enjoining RGW from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information; and compelling RGW to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety;

C. For an award of compensatory damages, punitive damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined;

D. For an award of attorneys' fees and costs, including expert witness fees;

E. Pre- and post-judgment interest on any amounts awarded; and

F. Such other and further relief as this court may deem just and proper

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all triable issues.

Dated: March 18, 2024

Respectfully Submitted,

/s/ Gary E. Mason
Gary E. Mason (MD Bar # 15033)
MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015
Tel: (202) 429-2290
Email: gmason@masonllp.com

Ben Barnow* (Interim Co-Lead Class Counsel)
Anthony L. Parkhill*
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Suite 1630
Chicago, IL 60606
Tel: 312-621-2000
Fax: 312-641-5504
Email: b.barnow@barnowlaw.com
Email: aparkhill@barnowlaw.com

Gary M. Klinger** (Interim Co-Lead Class Counsel)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel: 866-252-0878
Fax: 865-522-0049
gklinger@milberg.com

Tyler J. Bean* (Interim Co-Lead Class Counsel)
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, NY 10151
Tel: 212-532-1091
tbean@sirillp.com

Daniel O. Herrera**
Nickolas J. Hagman**
Mohammed A. Rathur**
CAFFERTY CLOBES MERIWETHER

& SPRENGEL LLP
135 S. LaSalle, Suite 3210
Chicago, Illinois 60603
Tel: 312-782-4880
dherrera@caffertyclobes.com
nhagman@caffertyclobes.com
mrathur@caffertyclobes.com

Kevin Laukaitis**
LAUKAITIS LAW LLC
954 Avenida Ponce De Leon, Suite 205, #10518
San Juan, PR 00907
Tel: 215-789-4462
klaukaitis@laukaitislaw.com

Ken Grunfeld**
KOPELOWITZ OSTROW FERGUSON WEISELBERG GILBERT
One West Las Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Telephone: 954-525-4100
grunfeld@kolawyers.com

William N. Sinclair
SILVERMAN THOMPSON SLUTKIN & WHITE, LLC
400 E. Pratt St., Suite 900
Baltimore, MD 21202
Tel: 410-385-222
Fax: 410-547-2432
bsinclair@silvermanthompson.com

Christopher D. Jennings**
JENNINGS, PLLC
P.O. Box 25972
Little Rock, Arkansas 72221
T: (501) 247-6267
E: chris@jenningspllc.com

Counsel for Plaintiffs and the Proposed Class

**pro hac vice*

***pro hac vice forthcoming*

CERTIFICATE OF SERVICE

I hereby certify that on this 18th day of March, 2024, I caused a true and correct copy of the foregoing to be filed with the Clerk of the Court via the Court's CM/ECF system, which will cause a copy to be electronically served upon all counsel of record.

/s/ Gary E. Mason
Gary E. Mason