DISTRICT COURT, ARAPAHOE COUNTY, STATE OF COLORADO Court Address: 7325 South Potomac St. Centennial, CO 80112	DATE FILED February 24, 2025 3:40 PM FILING ID: DEC25CC5871CF CASE NUMBER: 2025CV30456
Plaintiffs: Paula Henderson, Shykira Scott, Daniel Jones, Carol Goldberg, Vahram Haroutunian, Brian Kearney, Hilda Lopez, Preference Robinson, Sharon Etchieson, Radhe Banks, Jonathan Trusty, Marie Netrosio, Michaela Mujica-Steiner, Roger Loeb, Kyle Denlinger, Martin Coleman, Alyssa Halaseh, Rachel Hunter, Todd Valentine and David Moynahan, *on behalf of themselves and all others similarly situated*, v. **Defendants:** Reventics, LLC, OMH Healthedge Holdings, Inc., d/b/a Omega Healthcare	**▲ COURT USE ONLY ▲**
Attorney for Plaintiffs: Reid Elkus (CO. BAR #32516) **ELKUS & SISSON, P.C.** 7100 E Belleview Avenue, Suite 101 Greenwood Village, CO 80111 Tel: (303) 567-7981 Scott Edward Cole* (CA BAR #160744) **COLE & VAN NOTE** 555 12th Street, Suite 2100 Oakland, California 94607 Tel: (510) 891-9800 **Pro hac vice application forthcoming*	Case No.: Div.:
CLASS ACTION CIVIL COMPLAINT AND JURY DEMAND	

INTRODUCTION TO THE CASE

1. Plaintiffs Paula Henderson, Shykira Scott, Daniel Jones, Carol Goldberg, Vahram Haroutunian, Brian Kearney, Hilda Lopez, Preference Robinson, Sharon Etchieson, Radhe Banks, Jonathan Trusty, Marie Netrosio, Michaela Mujica-Steiner, Roger Loeb, Kyle Denlinger, Martin Coleman, Alyssa Halaseh, Rachel Hunter, Todd Valentine and David Moynahan (collectively, "Plaintiffs") bring this Class Action Complaint against Reventics, LLC ("Reventics") and OMH Healthedge Holdings, Inc. d/b/a Omega Healthcare ("Omega") (collectively "Defendants") on behalf of themselves, individually, and all others similarly situated ("Class Members") and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows.

2. Plaintiffs bring this class action against Defendants for their failure to properly secure and safeguard personally identifiable information ("PII")[1] and protected health information ("PHI")[2] including, but not limited to, first, middle and last names, addresses, dates of birth, Social Security Numbers, medical record numbers, patient account numbers, driver's license and other gvernment ID, healthcare providers' names and addresses, health plan names and health plan ID, clinical data including diagnosis information, dates of services, treatment costs, prescription medications, numeric codes used to identify services and procedures Plaintiffs received from their healthcare providers and a brief description of these codes (collectively, "PHI/PII").

3. With this action, Plaintiffs seek to hold Defendants responsible for the harms they caused and will continue to cause Plaintiffs and, potentially, millions[3] of other similarly situated persons in the large and preventable cyberattack purportedly discovered by Defendants on

---

[1] Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).

[2] Personal health information ("PHI") is a category of information that refers to an individual's medical records and history, which is protected under the Health Insurance Portability and Accountability Act. Inter alia, PHI includes test results, procedure descriptions, diagnoses, personal or family medical histories and data points applied to a set of demographic information for a particular patient.

[3] *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*, U.S. Dep't of Health & Hum. Servs., https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (follow the "Next" hyperlink at the bottom of the page to page 2) (last accessed May 15, 2023). On information and belief, Plaintiffs contend that the number of affected persons could be much higher.

December 15, 2022, by which cybercriminals infiltrated Defendants' inadequately protected network servers and accessed highly sensitive PHI/PII belonging to both adults and children, which was being kept insufficiently protected (the "Data Breach").

4. Plaintiffs further seek to hold Defendants responsible for not ensuring that the PHI/PII was maintained in a manner consistent with industry standards, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Privacy Rule (45 CFR, Part 160 and Parts A and E of Part 164), the HIPAA Security Rule (45 CFR Part 160 and Subparts A and C of Part 164),[4] among other relevant standards.

5. In February 2023, Reventics began notifying various state Attorneys General and many Class Members about a widespread Data Breach (via a "Notice of Data Security Incident") affecting its network systems. Reventics waited an excessive amount of time before issuing these notices, even though Plaintiffs and an extraordinary number of Class Members had very sensitive personal information accessed, exfiltrated and/or stolen,[5] causing them to suffer ascertainable losses in the form of, *inter alia*, the loss of the benefit of their bargain, the value of their time reasonably incurred to remedy or mitigate the effects of the attack, and the deprivation of their opportunity to take preventative action against identity theft and fraud.

6. Further, Defendants' Notice of Data Security Incident obfuscated the nature of the breach and the threat it posted—refusing to reveal how many people were impacted, how the breach happened, or why it took the Defendants so long to begin notifying victims that hackers had gained access to highly private information.

7. Specifically, while Defendants claim to have discovered the Data Breach as early as December 15, 2022, Defendants did not begin informing victims thereof until February 24, 2023, and failed to inform victims when or for how long the Data Breach occurred. Indeed, Plaintiffs and Class Members were unaware of the Data Breach until they received letters from Defendants informing them of its existence in late February or early March 2023, and more recently in May and June of 2023.

8. Plaintiffs, thus, bring this action on behalf of all persons whose PHI/PII was compromised as a result of Defendants' failure to: (i) adequately protect the PHI/PII of Plaintiffs and Class Members, (ii) warn Plaintiffs and Class Members of Defendants' inadequate information security practices, and (iii) effectively secure hardware containing protected PHI/PII using reasonable and effective security procedures free of vulnerabilities and incidents.

---

[4] Notably, Plaintiffs do not bring claims under HIPAA but, rather, allege that Defendants' failures to meet HIPAA standards serve as evidence of its negligence, generally.

[5] Jill McKeon, *Revenue Cycle Management Company Reports Healthcare Data Breach Impacting 250K*, Health IT Security (Feb. 24, 2023), https://healthitsecurity.com/news/revenue-cycle-management-company-reports-healthcare-data-breach-impacting-250k.

9. Plaintiffs and Class Members have suffered injury as a result of Defendants' conduct. These injuries include: (i) lost or diminished value of PHI/PII, (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud and/or unauthorized use of their PHI/PII, (iii) lost time and 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 substantially increased risk to their PHI/PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse, and (b) may remain backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PHI/PII.

10. Defendants disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly and/or negligently failing to take and implement adequate and reasonable measures to ensure that the PHI/PII of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PHI/PII of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they are, thus, entitled to injunctive and other equitable relief.

PARTIES

11. Plaintiffs are adult individuals who were notified by Defendants that their Private Information was impacted by the Data Breach and suffered harm as alleged herein.

12. Defendant Reventics LLC is a Delaware limited liability corporation with its principal place of business at 5575 DTC Parkway, Suite 125, Greenwood Village, CO 80111.[6] Under the guidance and leadership of Chief Executive Officer, Arnab Sen, Defendant Reventics commenced operations in 2015.[7] Defendant Reventics LLC provides software and support to improve clinical documentation and revenue cycle management.[8]

13. Defendant OMH Healthedge Holding Inc. USA, d/b/a Omega Healthcare ("Omega") is a Delaware corporation, headquartered in Boca Raton, Florida, and is a sophisticated company offering comprehensive software and support to physicians through its vast network of U.S.- and India-based healthcare services companies.

---

[6] *Summary*, Colo. Secretary of State, https://www.sos.state.co.us/biz/BusinessEntityDetail.do?quitButtonDestination=BusinessEntityResults&nameTyp=ENT&masterFileId=20151633989&entityId2=20151633989&fileId=20228098792&srchTyp=ENTITY (last visited May 3, 2023).

[7] *Id.*

[8] *About Us*, https://reventics.com/about (last visited May 3, 2023).

JURISDICTION AND VENUE

14. Defendants are headquartered and routinely conduct business in the State of Colorado where this Court is located, have sufficient minimum contacts in this State and have intentionally availed themselves of this jurisdiction by marketing and selling products and services, and by accepting and processing payments for those products and services within this State. Moreover, numerous class members reside and were impacted within the State of Colorado and within this County.

15. Venue is proper in this Court pursuant to Colorado Rules of Civil Procedure Rule 98 as Defendants reside in this Circuit and/or the causes of action emanate from actions or omissions occurring in Greenwood Village, Colorado.

FACTUAL ALLEGATIONS

Reventics LLC

16. Defendant Reventics LLC is a Delaware limited liability corporation with its principal place of business at 5575 DTC Parkway, Suite 125, Greenwood Village, CO 80111.[9] Under the guidance and leadership of Chief Executive Officer, Arnab Sen, Defendant Reventics commenced operations in 2015.[10] Defendant Reventics provides software and support to improve clinical documentation and revenue cycle management.[11]

17. Defendant Reventics solicits a wide array of sensitive patient data from physicians for analysis. Reventics requests and stores patient information such as medications, diagnoses, symptoms, billing codes, and dates of service.[12] Reventics aims to gather every possible piece of a patient's PHI/PII in order to analyze that patient's PHI/PII to produce billing codes and insights to increase returns on revenue per patient for the relevant physician or medical institution. In short, Reventics' business model relies near-exclusively on its ability to collect and monetize sensitive Class Member PHI/PII.

18. Reventics provides a Citrix web interface where physicians can upload patient data and/or link their electronic health records system to the Reventics web interface.[13]

---

[9] *Summary*, Colo. Secretary of State, https://www.sos.state.co.us/biz/BusinessEntityDetail.do?quitButtonDestination=BusinessEntityResults&nameTyp=ENT&masterFileId=20151633989&entityId2=20151633989&fileId=20228098792&srchTyp=ENTITY (last visited May 3, 2023).

[10] *Id.*

[11] *About Us*, https://reventics.com/about (last visited May 3, 2023).

[12] *Pre-encounter*, https://reventics.com/solutions/pre-encounter (last visited May 3, 2023); *RevCDI*, https://reventics.com/products/revcdi (last visited May 3, 2023).

[13] *Reventics reduces medical coding errors and claim-denial rates with Power Automate*, https://customers.microsoft.com/en-us/story/1402010266555191335-reventics-scales-capacity-and-improves-accuracy-in-healthcare-billing-service (last visited May 10, 2023).

Physicians and institutions using Reventics can even use an application on their personal phone to access Reventics services, as illustrated below.[14]

19. Once this patient data is uploaded and/or electronic health records linked via Reventics' web interface, Reventics stores the patient data on its servers.[15] Reventics then takes that stored data and, by utilizing its own software and the efforts of its United States and foreign-based medical coders, Reventics begins the process of analyzing the patient data.[16]

20. On information and belief, United States-based medical coders work in tandem with medical coders employed by Reventics Private Ltd., Defendant Reventics' overseas counterpart, located in Hyderabad, India.[17] Just like their American co-workers, these India-based medical coders analyze medical information gathered by Reventics. These India-based medical coders are typically paid the equivalent of $6,338.64 USD per year[18] and are told by

---

[14] Screenshot of Reventics' CDI Application as it functions on both Apple and Android phones. *Rev CDI* https://apps.apple.com/us/app/revcdi/id1446239671.

[15] *Id.*

[16] *Id.; Reventics Careers,* https://reventics.com/careers/india, https://reventics.com/careers/us (last visited May 10, 2023).

[17] https://www.ambitionbox.com/overview/reventics-overview. Reventics Private Ltd was incorporated on February 17, 2015, and currently employs 200-500 India citizens.

[18] By contrast, the average United States-based medical coder earns about $53,580 per year. This outsourcing of U.S. patient PHI/PII offshore clearly allows Reventics to reap massive profits. See, *Salary Expectations*, https://www.salary.com/research/salary/posting/medical-coder-salary#:~:text=How%20much%20does%20a%20Medical,falls%20between%20%2447%2C121%20and%20%2461%2C555 (last visited July 4, 2023); *Reventics Salaries*, https://www.ambitionbox.com/salaries/reventics-salaries (last visited July 4, 2023).

Defendant Reventics they will be coding least 60-70 US charts per day for "US Coding clients."[19]

21. Once medical coders translate the items in each patient's chart into billing codes for submission to insurance companies, Medicare, Medicaid, or directly to the patient for payment, payment requests are generated and submitted, e.g., to these insurance carriers or billed to the patient.[20] To track efficiencies and bolster its own profitability, Reventics further uses patient PHI/PII to build analytical models like the one pictured below to demonstrate which patient claims will likely be paid more quickly and more easily:[21]

22. At every step, Reventics collects, maintains, translates, analyzes, and compares sensitive patient PHI/PII and is well aware of its duty to protect that PHI/PII from unauthorized access. Indeed, Reventics advertises to its clients that its automation and coding services actually improve compliance with HIPAA and other healthcare privacy statutes,[22] a clear acknowledgement of its duties thereunder, not to mention an acknowledgement that confidentiality of patients' PHI/PII is a selling feature of Reventics' services and is of high importance to Class Members.

23. Indeed, in its Privacy Policy, Reventics promises that it "implement[s] measures

---

[19] *Id.*; *Reventics Job Descriptions*, https://www.ambitionbox.com/jobs/reventics-jobs (last visited July 4, 2023).

[20] Below is an image of the interface used to track patient payment statistics. *RevMax*, https://reventics.com/products/revcdi (last visited July 5, 2023).

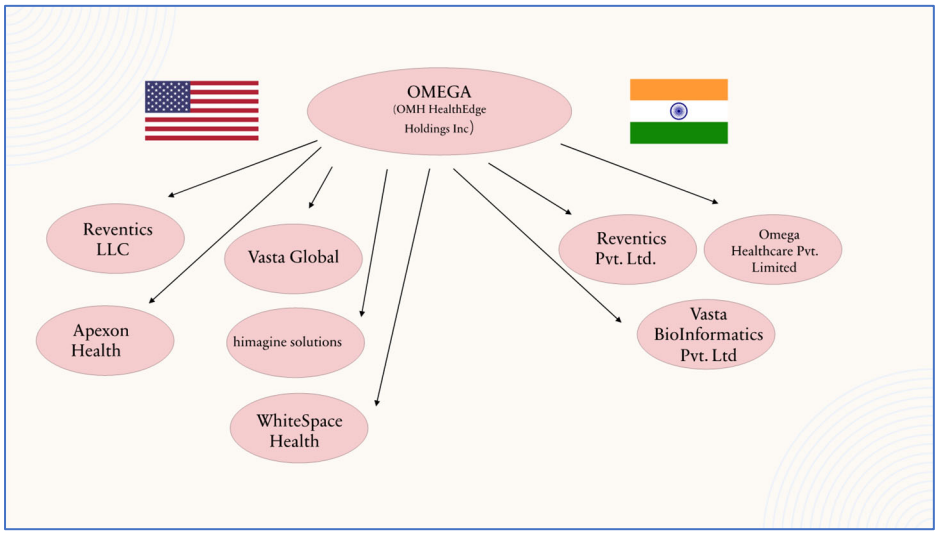
[21] *RevMax*, https://reventics.com/products/revcdi (last visited July 5, 2023).

[22] https://reventics.com/images/brochure/Softomotive_Reventics_Case_Study4444.pdf.

designed to secure your personal information from accidental loss and from unauthorized access, use, alteration, and disclosure." Thus, by Reventics' own Privacy Policy and advertising, Reventics explicitly promises that it will safeguard PHI/PII.

Omega

24. Defendant Omega is a Delaware corporation, headquartered in Boca Raton, Florida, and is a sophisticated company offering comprehensive software and support to physicians through its vast network of U.S. and India-based healthcare services companies. Omega has large ownership interest in (and/or wholly owns/controls), shares resources (including human resources) with, maintains interlocking management structures with, provides marketing services to, and commingles interests with various U.S.-based companies including Apexon Health, Vasta Global, HIMagine Solutions and WhiteSpace Health[23] and India-based companies including Vasta Bio-Informatics Private Limited and Omega Healthcare Management Private Limited. A current depiction of these relationships looks like:



25. Like Reventics, Omega is well aware of the sensitive nature of the Class Member PHI/PII it stores and analyzes for physicians insofar as it handles 16 percent of all emergency medicine charts in the United States and over 118 million medical charts annually.[24]

---

[23] *About Us*, https://www.omegahms.com/about-us/ (last visited May 3, 2023); *Omega Healthcare completes acquisition of ApexonHealth and Vasta Global* https://www.prnewswire.com/news-releases/omega-healthcare-completes-acquisition-of-apexonhealth-and-vasta-global-301524533.html (last visited May 3, 2023); *Omega Healthcare Acquires himagine Solutions*, Omega Healthcare (Mar. 17, 2021), https://www.omegahms.com/omega-healthcare-acquires-himagine-solutions/.

[24] *About Us*, https://www.omegahms.com/about-us/ (last visited May 3, 2023).

26. On March 8, 2022, OMH HealthEdge Holdings Inc. d/b/a Omega Healthcare acquired Defendant Reventics[25] in order to integrate Reventics' software and systems into its own portfolio of services.[26] "With the recently completed acquisition of Reventics, Omega Healthcare will deliver an end-to-end revenue cycle management suite of solutions to healthcare providers, from analytics-driven clinical documentation improvement to platforms for payment data management."[27] Put plainly, Omega sought to integrate Reventics' cloud-based software platforms into its own code and software offerings.[28]

27. In order to better effectuate the blending of the two companies, Reventics and Omega also combined leadership teams. At the time of the acquisition, Sumithra Gomatam, Executive Chair of Omega, stated "Omega is excited to welcome the Reventics team and is eagerly looking forward to creating enhanced value for its customers under the combined leadership."[29] After the merger, Arnab Sen, the founder and CEO of Reventics, transferred to Omega as its Chief Strategy Officer.[30] Similarly, Dr. David Friendson transferred from Chief Medical Officer at Reventics to the new Chief Medical Officer at Omega, and Vishalakshmi Tata transferred from her role as Vice President of Operations at Reventics to Vice President of Delivery at Omega.

28. Furthermore, according to the Indian Ministry of Corporate Affairs, in August 2022, five months after the merger, four directors from Omega's Board of Directors (namely, Sumithra Gomatam, Avinash Mehra, Suresh Vaswani and Anurag Singh Mehta) were added to Reventics Pvt. Ltd's Board of Directors as additional board members. Omega's Executive Board Chair even reviewed and signed Reventics Pvt. Ltd's audited financial report to the Indian Ministry of Corporate Affairs on October 28, 2022.

29. In addition to their combined and interlocking leadership, Omega has filed corporate documents directly on behalf of Reventics. Notably, its registered agent in Colorado changed to Maria Hursey, Omega's Contracts and Legal Operations Manager.[31] Additionally, Prateek Agrawal, Omega's Corporate Secretary has been listed as Reventics Pvt. Ltd's point of

---

[25] *Omega Healthcare expands capability in AI-based clinical documentation improvement* https://www.omegahms.com/omega-healthcare-acquires-reventics/ (last visited May 3, 2023).

[26] *Omega Healthcare expands capability in AI-based clinical documentation improvement https://www.omegahms.com/omega-healthcare-acquires-reventics/* (last visited May 3, 2023).

[27] *Omega Completes Acquisition* https://www.indianweb2.com/2022/04/omega-healthcare-completes-acquisition.html (last visited July 4, 2023).

[28] *Omega Acquires Reventics* https://en.prnasia.com/releases/apac/omega-healthcare-acquires-reventics-a-physician-focused-cdi-and-rcm-company-353876.shtml (last visited July 4, 2023).

[29] *Id.*

[30] *Leadership Team* https://www.omegahms.com/about-us/leadership/ (last visited July 4, 2023).

[31] *Statement of Change;* https://www.sos.state.co.us/biz/ViewImage.do?masterFileId=20151633989&fileId=20228202828 (last accessed July 4, 2023)

contact on the most recently filed November 23, 2022 FORM DIR 12 in Bangalore, India.[32]

30. Omega's acquisition of Reventics, as well as other recent companies like Vasta and Apexon, represents a larger goal of Omega to acquire companies that will position Omega as a one-stop shop for medical institutions and physicians. As C.E.O Anurag Mehta stated, "[t]hese partnerships are key steps towards making Omega Healthcare an all-compassing, digital-led, healthcare service provider."[33]

31. On information and belief, with these acquisitions, including its acquisition of Reventics, Omega collects and maintains patients' PHI/PII from every phase of their treatment through the subsequent billing.

32. Omega also directly interacts with patients through scheduling patient appointments and handling of patient calls. For example, one Omega employee generally schedules 45 to 50 patient appointments per day.[34] Next, Omega's staff and software handle the billing process by creating and submitting insurance authorizations, checking insurance eligibility, billing, medical coding, editing clinical documentation and submitting claims reimbursement to insurance.[35] Omega claims to have 7,000 medical coders who help clinics convert patient diagnoses and treatments into codes that insurance companies and government agencies use to authorize payments.[36] These coders (i.e., Reventics and Reventics Private Ltd staffers) view patient charts directly. Omega openly advertises that using their coders "reduce[s] costs" and "lowers overhead."[37]

33. Omega offers software and backend office support to help physicians and clinics work with Medicare patients.[38] Omega performs outreach (e.g., through phone calls) to chronically ill patients to remind them of appointments and necessary testing and obtain their medications.[39] Additionally, Omega audits its clients' patient data and evaluates whether more documentation is needed for Medicare/Medicaid reporting and/or reimbursement. In so doing, Omega regularly works with millions of patients in the United States each year. Omega claims

---

[32] *Data Breach Notifications* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed July 4, 2023)

[33] *Omega Announces Strategic Acquisitions* https://www.expresscomputer.in/news/omega-healthcare-announces-strategic-acquisitions-to-strengthen-its-tech-enabled-services/85797/ (last visited July 4, 2023).

[34] *Patient Access* https://www.omegahms.com/patient-access-services/ (last visited July 4, 2023).

[35] *Id.*

[36] *Omega Mid-Cycle Services* https://www.omegahms.com/mid-cycle-services/ (last visited July 4, 2023).

[37] *Id.*

[38] *Payer Administrative Services* https://www.omegahms.com/payer-administrative-services/ (last visited July 4, 2023).

[39] *Id.*

that "registered nurses" perform clinical chart reviews to code medical charts for Medicare and Medicaid reimbursements. Finally, Omega regularly answers and receives an estimated 8,000,000 patient calls and emails in connection with its patient outreach service.[40]

34. Omega provides both software and backend office support to help physicians secure approval for medications. Omega receives pharmacy requests and insurance authorizations for medications on behalf of physicians. Omega either automates this process with technology or Omega's staff directly submits the paperwork on behalf of the physician. Omega also monitors patients currently taking medications by proactively contacting patients through "a team of highly skilled clinicians, 90% of whom are registered nurses."[41]

35. Omega offers software and backend support to manage clinical research. Omega analyzes and cleans up data from clinical trials to submit to government agencies for approval and takes data from patient charts to demonstrate off-label uses of drugs for FDA approval. Omega is currently managing 500 clinical trials.[42]

36. Through every feature of Omega's operations, it handles PHI/PII for millions of Americans, whether they are aware of it or not. Given the sheer volume and depth of Omega's involvement in the American medical system, Omega was aware of its duties to protect the PHI/PII in its custody, including that of its subsidiary, Reventics. In fact, in recent months, Omega has bragged about its cybersecurity credentials and has even, most recently, celebrated data privacy day.[43] Omega has also publicly touted its recent achievement of HiTrust Certification.[44] Despite its claimed emphasis on data privacy and certifications, however, Omega's protection of the PHI/PII of Plaintiffs and the Class was abysmal.

37. Upon the above information and belief, (1) Omega owns all or majority of the capital stock of Reventics; (2) Omega and Reventics have common directors or officers; (3) Omega finances Reventics; (4) Omega subscribes to all the capital stock of Reventics or otherwise causes its incorporation; (5) Reventics has grossly inadequate capital; (6) Omega pays the salaries or expenses or losses of Reventics; (7) Reventics has substantially no business except with Omega or no assets except those conveyed to it by Omega; (8) in the papers of Omega, and in the statements of its officers, Reventics is referred to as a subsidiary; (9) the directors or executives of Reventics do not act independently in the interest of Reventics but take direction

---

40 *Id.*

41 *Id.*

42 *Clinical Data Services*, https://www.omegahms.com/clinical-data-services/ (last visited July 8, 2023).

43 *Data Privacy Day*, https://www.linkedin.com/posts/omega-healthcare-management-services_dataprivacyday-cybersecurity-datasecurity-activity-7025100233755791360-bBH1/?originalSubdomain=gh (last visited July 8, 2023).

44 https://www.omegahms.com/omega-healthcare-achieves-hitrust-implemented/ (last visited July 8, 2023).

from Omega; (10) Omega does not observe the formal legal requirements of Reventics as a separate and independent corporation.

The Data Breach

38. On December 15, 2022, Reventics discovered that cybercriminals accessed and encrypted its network.[45]

39. On December 27, 2022, a cybersecurity firm determined cybercriminals accessed and exfiltrated patients' PHI/PII from Reventics' servers, including, but not limited to, names, addresses, dates of birth, Social Security numbers, medical record numbers, patient account numbers, financial information, driver's licenses, government issued identification cards, healthcare provider information, health plan information, diagnosis information, dates of service, treatment costs, and prescription medications.[46]

40. On February 10, 2023, Reventics reported to the Department of Health and Human Services that cybercriminals accessed over 250,918 patient records.[47]

41. On February 13, 2023, Royal Ransomware, a well-known cybercriminal group, added Reventics to its list of victims on its Dark Web Access page. Royal Ransomware then leaked more than 16 GB of patient files held by Defendants, which Royal claimed was merely 10 percent of what it exfiltrated.[48] 16 GB is approximately to 300,000 pages of information.[49]

42. Royal Ransomware first appeared on the cybercrime scene in early 2022.[50] Royal Ransomware is known for a double extortion technique by which it typically encrypts the target

---

45 *Notice of Data Security Incident-Reventics*, https://www.doj.nh.gov/consumer/security-breaches/documents/reventics-20230303.pdf (last visited May 3, 2023).

46 *Reventics Experiences Data Security Incident*, Regional One Health (Feb. 14, 2023), https://www.regionalonehealth.org/blog/2023/02/14/reventics-experiences-data-security-incident/ (last visited May 17, 2023).

47 *Breach Portal*, *supra* note 3.

48 *Reventics notifying patients of ransomware incident*, DataBreaches.net, (Feb. 19, 2023), https://www.databreaches.net/reventics-notifying-patients-of-ransomware-incident/.

49 *Additional Storage Capacity*, https://www.memorysuppliers.com/blogs/memory-suppliers-blog/what-usb-flash-drive-capacity-do-you-really-need#:~:text=16GB%20%E2%80%93%20can%20hold%20approximately%2010240,or%205120%20minutes%20of%20video (last visited May 3, 2023).

50 Shunichi Imano & James Slaughter, *Royal Ransomware Round Up*, Fortinet.com/blog (Oct. 13, 2022), https://www.fortinet.com/blog/threat-research/ransomware-roundup-royal-ransomware.

organization's data and then exfiltrates that data.[51] Royal then, typically, demands a ransom of $250,000 to $2 million dollars.[52]

43. Prior to the Data Breach, the Office of Information Security within the Department of Health Human Services released a report to warn healthcare providers about Royal Ransomware[53] and its techniques, explaining that Royal Ransomware was known to use ransomware to target the healthcare community. In every attack prior to the Data Breach, Royal Ransomware claimed to have published 100 percent of the data that was allegedly extracted from the victim.[54]

44. Royal Ransomware uses a 64-bit executable code that targets Windows systems, which, upon information and belief, makes up a majority of Reventics' architecture.[55] Royal Ransomware usually infects computer systems via phishing, a technique whereby its cybercriminals create fake installer notifications, links, emails, or ads that entice unsuspecting users to click and thereby infect their computers.[56]

45. On or around February 24, 2023, Defendants began disseminating their Notice of Data Security Incident to Plaintiffs and Class Members. As of that time, roughly 250,918 potentially affected individuals were sent Notices of the Breach.

46. According to the Notice of Data Security Incident, on or about December 15, 2022, Reventics claims to have "detected certain anomalies in its systems, including a cyber-intruder who encrypted and potentially accessed Sensitive Information on Reventics' servers." Defendants further acknowledged that "[c]ertain personally identifiable information ("PII") and Protected Health Information protected under HIPAA and state privacy laws was contained on Reventics' systems and was impacted by the breach."

47. The Notice of Data Security Incident admits that "[o]n or about December 27, 2022, it was determined that unauthorized acquisition of information had occurred." The further Notice of Data Security Incident sent to Plaintiffs and Class Members also claimed the following PHI/PII was impacted by the Data Breach:

---

[51] *Id.*

[52] *HC3: Analyst Note: Royal Ransomware*, U.S. Dept. of Health & Hum. Servs., https://www.hhs.gov/sites/default/files/royal-ransomware-analyst-note.pdf (last visited July 8, 2023).

[53] *HC3: Analyst Note: Royal Ransomware*, U.S. Dep't of Health & Hum. Servs., https://www.hhs.gov/sites/default/files/royal-ransomware-analyst-note.pdf (last visited May 3, 2023).

[54] *Id.*

[55] *Id.*

[56] *DEV 0569 Finds New Way to Deliver Royal Ransomware*, https://www.microsoft.com/en-us/security/blog/2022/11/17/dev-0569-finds-new-ways-to-deliver-royal-ransomware-various-payloads/; *#STOP Ransomware: Royal Ransomware* https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a (last visited July 8, 2023).

> [F]irst, middle and last name, address, date of birth, medical record number, patient account number, driver's license and other government issued ID, healthcare provider's name and address, health plan name and health plan ID, clinical data including diagnosis information, dates of services, treatment costs, prescription medications, the numeric codes used to identify services and procedures you received from your healthcare provider and a brief description of these codes.

48. On or around February 23, 2023, an update to the Data Breach notification was posted on Reventics' website that disclosed additional categories of information not already included in the Notice(s) of Data Breach previously sent to Plaintiffs and Class Members.[57] The additional information disclosed included further forms of Plaintiff and Class Member PHI/PII. That version of the Notice stated the following in pertinent part:

> On December 27, 2022, the cybersecurity and forensic consulting firm confirmed that the cyber-intruder accessed and exfiltrated certain personally identifiable information ("PII") and Protected Health Information ("PHI") protected under HIPAA and state privacy laws. This information included first and last name, date of birth, social security number, financial information, healthcare provider's name and address, health plan name, clinical data, the numeric codes used to identify services and procedures patients received from healthcare providers and a brief description of these codes.[58]

49. On information and belief, however, Plaintiffs allege the scope of PHI/PII exfiltrated was far more expansive than these examples suggest. Plaintiffs further allege that, altogether, several waves of Notices have been issued to impacted Class Members, as Defendants continue to uncover the identity of additional persons affected by the Data Breach.

50. In response to the Data Breach, Reventics contends that it has or will be working: "diligently with their third-party cybersecurity consultants to further fortify Reventics' systems."[59] Although Reventics fails to expand on what these alleged "further" fortifications and safeguards are, such fortifications and safeguards could and should have been in place before the Data Breach.

51. Through its Notice of Data Security Incident (and subsequent iterations thereof), Reventics also acknowledged the actual imminent harm and injury that flowed from the Data Breach, thus encouraging breach victims to "remain vigilant by reviewing account statements

---

[57] *Reventics Notifying Patients of Ransomware Incident*, DataBreaches.net (Feb. 19, 2023), https://www.databreaches.net/reventics-notifying-patients-of-ransomware-incident/.

[58] https://reventics.com/images/email-images/notice-of-data-security-incident.png (last visited May 15, 2023).

[59] *Id.*

and monitoring credit reports."[60] Plaintiffs and Class Members would otherwise have had no reason to do so, demonstrating one of the elements of harm and injury alleged herein. Moreover, by encouraging such actions, Defendants are estopped from contending Plaintiffs' and Class Members' protective actions were unnecessary, unwise, or unwarranted.

52. In addition to the Notice(s) by Reventics, medical institutions have similarly disclosed that they were customers of Reventics and, thus, may have patients affected by the Data Breach. The medical institutions include Regional One, Emergency Medical Specialists of Colorado, and Great Falls Hospital,[61] just to name a few.

53. On May 5, 2023, Reventics stated it had concluded its investigation of the Data Breach. However, as of this filing, Reventics has yet to disclose any report generated as a result of the investigation.

54. As a result of the Data Breach, Plaintiffs and numerous Class Members suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack, not to mention the substantial and imminent risk of identity theft.

55. As a result of Defendants' delayed response, Plaintiffs and Class Members had no idea their PHI/PII 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. These risks will remain for their respective lifetimes.

56. Defendants' failure to timely detect and report the Data Breach made their consumers vulnerable to identity theft without any prior warning to monitor their financial accounts or credit reports to prevent unauthorized use of their PHI/PII.

57. The PHI/PII compromised in connection with the Data Breach was due to Defendants' negligent and/or careless acts and omissions and their failure to protect the PHI/PII of Plaintiffs and Class Members. In addition to Defendants' failure to prevent the Data Breach, after discovering it, Defendants waited months to report it to government agencies and affected individuals.

58. On information and belief, despite recognizing their duty to do so, Defendants have not implemented reasonable cybersecurity safeguards or policies to protect their consumers' PHI/PII or trained their IT or data security employees to prevent, detect and stop breaches of their systems. As a result, Defendants leave significant vulnerabilities in their systems for cybercriminals to again exploit and gain access to consumers' PHI/PII.

---

[60] *Id.*

[61] https://www.regionalonehealth.org/blog/2023/02/14/reventics-experiences-data-security-incident/; https://www.gfclinic.com/security-incident-at-reventic-a-great-falls-clinic-vendor/; https://coloradoemspc.com (last visited July 8, 2023).

59. Plaintiffs and Class Members directly or indirectly entrusted Defendants with sensitive and confidential information, including their PHI/PII, which includes information that is static, does not change and can be used to commit myriad financial crimes.

60. Plaintiffs and Class Members relied on Defendants to keep their PHI/PII confidential and securely maintained, to use this information only for purposes benefitting Plaintiffs and Class Members, and to make only authorized disclosures of this information.

61. The unencrypted PHI/PII of Plaintiffs and Class Members will likely end up for sale on the dark web, as that is the *modus operandi* of hackers. In addition, unencrypted PHI/PII may fall into the hands of companies that will use the PHI/PII for targeted marketing without the approval of Plaintiffs and Class Members. Thus, unauthorized individuals can, and undoubtedly will, easily access the PHI/PII of Plaintiffs and Class Members.

62. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiffs and Class Members, causing the exposure of the PHI/PII.

Defendants Had an Obligation to Protect the Private Information

63. Defendants' failure to adequately secure Plaintiffs and Class Members' PHI/PII violated duties Defendants owed Plaintiffs and Class Members under common law. Under HIPAA, health insurance providers have an affirmative duty to keep patients' Protected Health Information private. As covered entities, Defendants held a duty under HIPAA to safeguard Plaintiffs and Class Members' data. Moreover, Plaintiffs and Class Members surrendered their highly sensitive personal data to Defendants under the implied condition that Defendants would keep it private and secure. Accordingly, Defendants also had an implied duty to safeguard their data, independent of any statute.

64. Because Defendants are covered by HIPAA (45 C.F.R. § 160.102), they are required to comply with the HIPAA Privacy 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.

65. HIPAA's Privacy Rule and Security Rule establish national standards for the protection of health information, including a set of security standards for protecting health information that is kept or transferred in electronic form.

66. HIPAA requires Defendants to "comply with the applicable standards, implementation specifications and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

67. "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.

68. HIPAA's Security Rule requires Defendants to:

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 [their] workforce[s].

69. HIPAA also requires Defendants to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information" under 45 C.F.R. § 164.306(e) and 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).

70. Moreover, the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, required Defendants 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." Defendants breached this duty.

71. Defendants were also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. S*ee, e.g.*, *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

72. In addition to their obligations under federal and state laws, Defendants owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PHI/PII in Defendants' possession from being compromised, lost, stolen, accessed, and/or misused by unauthorized persons. Defendants owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems,

networks, and protocols adequately protected the PHI/PII of Plaintiffs and Class Members.

73. Defendants also owed a duty to Plaintiffs and Class Members to design, maintain, and test their computer systems, servers, and networks to ensure that the PHI/PII in their possession was adequately secured and protected.

74. Defendants also owed a duty to Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect the PHI/PII in their possession, including not sharing information with entities who maintained substandard data security systems.

75. Defendants also owed a duty to Plaintiffs and Class Members to implement processes that would immediately detect a breach on their data security systems in a timely manner.

76. Defendants also owed a duty to Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

77. Defendants also owed a duty to Plaintiffs and Class Members to disclose if their computer systems and data security practices were inadequate to safeguard individuals' PHI/PII from theft because such an inadequacy would be a material fact in the decision to entrust this PHI/PII to Defendant.

78. Defendants also owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

79. Finally, Defendants owed a duty to Plaintiffs and Class Members to encrypt and/or more reliably encrypt Plaintiffs' and Class Members' PHI/PII and monitor user behavior and activity in order to identify possible threats.

DEFENDANTS' FAILURES

The Data Breach Was Foreseeable

80. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PHI/PII of Plaintiffs and Class Members, and the foreseeable consequences that would occur if Defendants' data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

81. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' network, amounting to, potentially, millions of personal records and, thus, the significant number of individuals who would be harmed by the

exposure of the seemingly unencrypted data.

Value of PII/PHI, Generally

82. The PHI/PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200 and bank details have a price range of $50 to $200.[62] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[63] Criminals can also purchase access to an entire company's data breach records for a sum of $900 to $4,500.[64]

83. 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 scenarios because, in those cases, victims can cancel or close credit and debit card accounts. Commonly, the information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

84. 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."[65]

85. 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.

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

87. Theft of PHI is also gravely serious: a thief may use a person's name or health insurance numbers to see a doctor, get prescription drugs, file claims with insurance providers, or

---

62 Anita George, *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/ (last visited May 17, 2023).

63 Brian Stack, *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/ (last accessed May 17, 2023).

64 *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited May 17, 2023).

65 Time 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.

obtain other forms of care.[66] "If the thief's health information is mixed with yours, your treatment, insurance and payment records and credit report may be affected."[67]

88. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PHI/PII on the black market for the purpose of target marketing their products and services based upon the physical maladies of the data breach victims themselves. Insurance companies even purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

89. Moreover, there may be a time lag between when a data breach occurs and when it is discovered, and between when PHI/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.[68]

90. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PHI/PII of Plaintiffs and Class Members, including their PHI/PII, and of the foreseeable consequences that would occur if Defendants' data security systems were breached, including the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

91. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, its monitoring, and the loss of other rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of its PHI/PII.

92. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' network, amounting to, potentially, millions of personal records and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

93. To date, Defendants have offered Plaintiffs and Class Members only 12 months of identity and credit monitoring services through IDX, a purported remedy already offered in

---

66 *See What to Know About Medical Identity Theft*, Fed. Trade Comm'n (2021), https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last visited May 17, 2023).

67 *Id.*

68 *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited May 17, 2023).

connection with nearly every data breach in the nation. But this offered service is inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of the kind of PHI/PII at issue here. Moreover, Defendants put the burden squarely on Plaintiffs and Class Members to enroll in these inadequate monitoring services.

Defendants Failed to Properly Protect Plaintiffs' and Class Members' Private Information

94. Defendants could have prevented this Data Breach by properly securing and encrypting the systems containing the PHI/PII of Plaintiffs and Class Members. Alternatively, Defendants could have destroyed the data, especially for individuals with whom they had not had a relationship for a reasonable period of time.

95. Defendants' negligence in safeguarding the PHI/PII of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to companies like Defendants to protect and secure the kind of sensitive data they possessed.

96. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 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."[69] Defendants should have been aware of the scope of such sensitive information and the impact their disclosure would, naturally, have on Plaintiffs and Class Members.

97. In light of this, and so as to prevent and detect unauthorized cyber-attacks, Defendants 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

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

files from reaching end users;

- Configure firewalls to block access to known malicious IP addresses;
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system;
- Set anti-virus and anti-malware programs to conduct regular scans automatically;
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary;
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories or shares;
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications;
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder;
- Consider disabling Remote Desktop protocol (RDP) if it is not being used;
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy;
- Execute operating system environments or specific programs in a virtualized environment; and
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[70]

98. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendants could and should also 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

[70] *Id.* at 3-4.

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.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls and email filters—and keep them updated—to reduce malicious network traffic….[71]

99. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendants could and should also 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

[71] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://www.cisa.gov/news-events/news/protecting-against-ransomware.

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

Include IT Pros in security discussions

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

Build credential hygiene

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

Apply principle of least-privilege

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

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[72]

100. The occurrence of the Data Breach indicates that Defendants failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PHI/PII of Plaintiffs and Class Members.

101. And yet, because Defendants failed to properly protect and safeguard Plaintiffs' and Class Members' PHI/PII, an unauthorized third party was able to access Defendants' network and access Defendants' database and system configuration files and exfiltrate that data.

Defendants Failed to Comply with Industry Standards

102. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the PHI/PII they collect and maintain.

---

[72] *See Human-operated ransomware attacks: A preventable disaster*, Microsoft (Mar. 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

103. Several best practices have been identified that, at a minimum, should be implemented by healthcare service providers like Defendants, 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.

104. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software, monitoring and limiting the network ports, protecting web browsers and email management systems, setting up network systems such as firewalls, switches and routers, monitoring and protection of physical security systems, protection against any possible communication system, and training staff regarding critical points.

105. Defendants 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), all of which are established standards for reasonable cybersecurity readiness.

106. The foregoing frameworks are existing and applicable industry standards in the healthcare industry, but Defendants failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

Defendants' Negligent Acts and Breaches

107. Defendants participated in and controlled the process of gathering the PHI/PII from Plaintiffs and Class Members.

108. Defendants, therefore, assumed and otherwise owed duties and obligations to Plaintiffs and Class Members to take reasonable measures to protect the information, including the duty of oversight, training, instruction, testing of the data security policies and network systems. Defendants breached these obligations to Plaintiffs and Class Members and/or were otherwise negligent because they failed to properly implement data security systems and policies for their health providers network that would adequately safeguarded Plaintiffs' and Class Members' sensitive information. Upon information and belief, Defendants' unlawful conduct included, but was not limited to, one or more of the following acts and/or omissions:

a. Failing to design and maintain an adequate data security system to reduce the risk of data breaches and protect Plaintiffs' and Class Members sensitive information;

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

c. Failing to test and assess the adequacy of their data security system;

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

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

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

g. Failing to ensure or otherwise require that they were compliant with FTC guidelines for cybersecurity;

h. Failing to ensure or otherwise require that they were adhering to one or more of industry standards for cybersecurity, as discussed above;

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

j. Failing to require encryption or adequate encryption on their data systems; and

k. Otherwise negligently and unlawfully failing to safeguard Plaintiffs' and Class Members' PHI/PII provided to Defendants which, in turn, allowed cyberthieves to access their IT systems.

COMMON INJURIES AND DAMAGES

109. As result of Defendants' ineffective and inadequate data security practices, Plaintiffs and Class Members now face a present and ongoing risk of fraud and identity theft.

110. Due to the Data Breach and the foreseeable consequences of PHI/PII ending up in the possession of criminals, the risk of identity theft to Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy, (b) "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft, (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk, (d) "out of pocket" costs incurred due to actual identity theft, (e) loss of time incurred due to actual identity theft, (f) loss of time due to increased spam and targeted marketing emails, (g) the loss of benefit of the bargain, (h) diminution of value of their PHI/PII, and (i) the continued risk to their PHI/PII, which remains in Defendants' possession and which is subject to further breaches, so

long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PHI/PII.

The Risk of Identity Theft to Plaintiffs and Class Members Is Present and Ongoing

111. The link between a data breach and the risk of identity theft is simple to grasp and well established: Criminals acquire and steal PHI/PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes, as discussed further below.

112. Because a person's identity is akin to a puzzle with multiple data pieces, 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 track the victim so as to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

113. 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 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 and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on victims.

114. The dark web is an unindexed layer of the internet that requires special software or authentication to access.[73] Criminals, in particular, favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or "surface" web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov but, on the dark web, the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[74] This anonymity prevents dark web marketplaces from being easily monitored by authorities or accessed by less sophisticated users.

115. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs and frequently, personal, and medical information like the PHI/PII at issue here.[75] The digital character of PHI/PII stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet while the buyer and seller retain their anonymity. The sale of a firearm or drugs, on the other hand, requires a physical

[73] Louis DeNicola, *What Is the Dark Web?*, Experian (May 12, 2021), https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.

[74] *Id.*

[75] *What is the Dark Web?* – Microsoft 365 (July 15, 2022), https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.

delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials and Social Security numbers, dates of birth and medical information.[76] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[77]

116. Social Security numbers, for example, are among the most devastating kind of PII to have stolen because they may be put to numerous serious fraudulent uses and are difficult for individuals to change. The Social Security Administration stresses that the loss of Social Security numbers, as occurred 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.[78]
>
> What's 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.

117. Even then, obtaining a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[79]

118. 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 jobs using stolen Social

---

76 *Id.*; *see also* Louis DeNicola, *supra* note 82.

77 *What is the Dark Web?* – Microsoft 365 (July 15, 2022), https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web.

78 Social Security Administration, *Identity Theft and Your Social Security Number* (2021), available at: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited May 17, 2023).

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

Security numbers, rent houses or receive medical services in the victims' names, and may even give that personal information to police during arrests resulting in arrest warrants being issued in victims' names. The Social Security Administration has further warned that identity thieves can use stolen Social Security numbers to apply for additional credit lines.[80]

119. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[81]

120. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[82] Defendants, however, did not rapidly report to Plaintiffs and/or the Class that their PHI/PII had been stolen.

121. Victims of identity theft also often suffer embarrassment, blackmail or harassment—in person or online, and/or experience financial losses resulting from fraudulently opened accounts or the misuse of existing accounts.

122. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims spend a considerable time repairing the damage caused by the theft of their PHI/PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones and/or dispute charges with creditors.

123. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen private information. To protect themselves, Plaintiffs and Class Members must, therefore, remain vigilant against unauthorized data use for years or even decades to come.

124. The Federal Trade Commission ("FTC") has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses or why their information may be commercially valuable. Data is currency. Thus, the larger the data set, the greater potential for analysis and profit."[83]

---

80 *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2021), https://www.ssa.gov/pubs/EN-05-10064.pdf. (last visited May 17, 2023).

81 *See 2019 Internet Crime Report*, FBI (Feb. 11, 2020), https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120.

82 *Id.*

83 Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring

125. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making. According to the FTC, data security requires: (1) encrypting information stored on computer networks, (2) retaining payment card information only as long as necessary, (3) properly disposing of personal information that is no longer needed, (4) limiting administrative access to business systems, (5) using industry-tested and accepted methods for securing data, (6) monitoring activity on networks to uncover unapproved activity, (7) verifying that privacy and security features function properly, (8) testing for common vulnerabilities, and (9) updating and patching third-party software.[84]

126. According to the FTC, unauthorized PII disclosures are extremely damaging to consumers' finances, credit history and reputation and can take time, money and patience to resolve the fallout. The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.[85]

127. Defendants' failure to properly and timely notify Plaintiffs and Class Members of the Data Breach exacerbated Plaintiffs' and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their PHI/PII and take other necessary steps to mitigate the harm caused by the Data Breach.

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

128. As a result of the recognized risk of identity theft, when a Data Breach occurs and an individual is notified by a company that his/her PHI/PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm. In working to protect against future identity theft or fraud, however, an individual suffers harm to a different, but no less valuable, asset: time itself.

129. Thus, due to the actual and imminent risk of identity theft, Plaintiffs and Class Members must, as Defendants' Notice of Data Security Incident instructs them, "remain vigilant by reviewing [their] account statements and monitoring credit reports."

Privacy Roundtable), FTC (Dec. 7, 2009), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf.

[84] *See generally* https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited May 17, 2023).

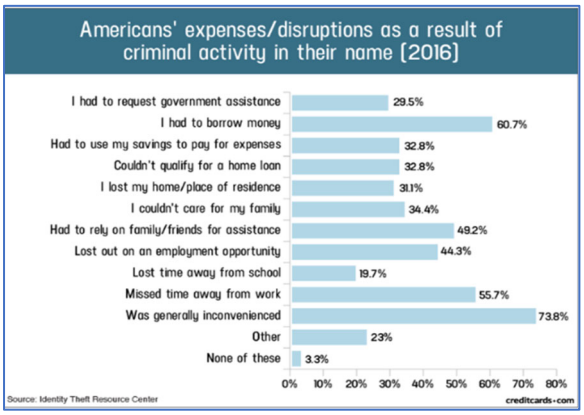
[85] *See, e.g.*, *Protecting Personal Information: A Guide for Business*, FTC, https://www.ftc.gov/news-events/news/press-releases/2016/07/commission-finds-labmd-liable-unfair-data-security-practices (last visited May 15, 2023).

130. Plaintiffs and Class Members have spent and will spend additional time in the future on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing, or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover and detect.

131. Plaintiffs' and Class Members' mitigation efforts are consistent with the U.S. Government Accountability Office's 2007 report regarding data breaches ("GAO Report"), in which the GAO noted that victims of identity theft will undoubtedly face "substantial costs and time to repair the damage to their good name and credit record."[86]

132. Plaintiffs' and Class Members' mitigation efforts are also consistent with the steps that the 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 (and 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.[87]

133. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[88]



86 *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-07-737, PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN (2007) ("GAO Report"), available at https://www.gao.gov/new.items/d07737.pdf (last visited May 17, 2023).

87 *See* Federal Trade Commission, IdentityTheft.gov, https://www.identitytheft.gov/Steps (last visited July 10, 2023).

88 Jason Steele, *Credit Card and ID Theft Statistics* (Oct. 24, 2017), https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276 (last visited May 17, 2023).

134. 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."[89] Indeed, the FTC recommends that identity theft victims take several steps and spend time 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.[90]

Diminution of Value of the Private Information

135. Undisclosed PII and/or PHI are valuable property rights.[91] Their value is axiomatic, considering the consequences for theft of that data. Even this obvious risk-to-reward analysis illustrates beyond doubt that PHI and/or PII has considerable market value.

136. For example, drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PHI/PII on the black market for the purpose of target-marketing their products and services.

137. Sensitive PHI/PII can sell for as much as $363 per record, according to the Infosec Institute.[92] According to account monitoring company, LogDog, medical data, such as PHI, sells for $50 and up on the Dark Web.[93]

138. An active and robust legitimate marketplace for private information like PII and/or PHI also exists. In 2019, the data brokering industry was worth roughly $200 billion.[94] In

---

89 *See* GAO Report, *supra* note 95, at 2.

90 *See* Federal Trade Commission, IdentityTheft.gov, https://www.identitytheft.gov/Steps (last visited May 19, 2023).

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

92 *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/.

93 Lisa Vaas, *Ransomware Attacks Paralyze and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content.

94 David Lazarus, *Column: Shadowy data brokers make the most of their invisibility cloak*, LA Times (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers.

fact, the data marketplace is so sophisticated that consumers can sell their non-public information directly to a data broker who, in turn, aggregates the information and provides it to marketers or app developers.[95,96] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[97]

139. As a result of the Data Breach, Plaintiffs' and Class Members' PHI/PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished in its value by its unauthorized and potential release on the Dark Web, where it holds significant value for the threat actors.

Injunctive Relief Is Necessary to Protect against Future Data Breaches

140. Moreover, Plaintiffs and Class Members have an interest in ensuring that their PHI/PII, which is believed to remain in the possession of Defendants, is protected from further breaches by the implementation of security measures and safeguards, including, but not limited to, ensuring that the storage of data or documents containing PHI/PII is not accessible online and that access to such data is password protected.

CLASS ALLEGATIONS

141. Plaintiffs bring this class action on behalf of themselves and on behalf of all others similarly situated pursuant to Colorado Rules of Civil Procedure Rule 23. Plaintiffs seek to represent the following Class:

> **Nationwide Class**
>
> All United States residents whose Private Information was potentially exposed to unauthorized third parties as a result of the data breach allegedly discovered by Defendant on or before December 15, 2022. (the "Nationwide Class" or simply the "Class").

142. Excluded from the Class are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers, and directors and any entity in which Defendants have a controlling interest, all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, any and all federal, state or local governments, including, but not limited to, their departments, agencies, divisions, bureaus, boards, sections, groups, counsels, and/or subdivisions and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

---

95 https://datacoup.com/ (last visited May 17, 2023).

96 https://digi.me/what-is-digime/.(last accessed May 17, 2023).

97 Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last accessed May 15, 2023).

143. Plaintiffs reserve the right to modify or amend the definition(s) of the proposed Class before the Court determines whether certification is appropriate.

144. Numerosity: Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are as many as several million members of the Class.

145. Commonality: Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendants had a duty to protect the PHI/PII of Plaintiffs and Class Members;

b. Whether Defendants had duties not to disclose the PHI/PII of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendants had duties not to use the PHI/PII of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendants failed to adequately safeguard the PHI/PII of Plaintiffs and Class Members;

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

f. Whether Defendants adequately, promptly, and accurately informed Plaintiffs and Class Members that their PHI/PII had been compromised;

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

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

i. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PHI/PII of Plaintiffs and Class Members;

j. Whether Plaintiffs and Class Members are entitled to actual, consequential and/or nominal damages as a result of Defendants' wrongful conduct;

k. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendants' wrongful conduct; and

l. Whether Plaintiffs and Class Members are entitled to injunctive relief to

redress the imminent and currently ongoing harm faced as a result of the Data Breach.

146. Typicality: Plaintiffs' claims are typical of those of other Class Members because all had their PHI/PII compromised as a result of the Data Breach, due to Defendants' misfeasance.

147. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge to these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

148. Adequacy: Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the remaining Class Members and the infringement of the rights and the damages Plaintiffs have suffered are typical of other Class Members. Plaintiffs have also retained counsel highly experienced in complex class action litigation and Plaintiffs intend to prosecute this action vigorously.

149. Superiority and Manageability: Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently and without the unnecessary duplication of evidence, effort and expense that numerous individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

150. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because (a) Defendants would otherwise necessarily gain an unconscionable advantage in that they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources, (b) the costs of individual suits could unreasonably consume the amounts that would be recovered, (c) proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged, and (d)

individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

151. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, consistent relevant laws and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

152. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

153. Unless a Class-wide injunction is issued, Defendants may continue in their failure to properly secure the PHI/PII of Class Members, Defendants may continue to refuse to provide proper notification to Class Members regarding the Data Breach and Defendants may continue to act unlawfully, as set forth in this Complaint.

154. Further, Defendants have acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Colorado Rules of Civil Procedure Rule 23.

155. Likewise, particular issues under Colorado Rules of Civil Procedure Rule 23 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 Defendants owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PHI/PII;

b. Whether Defendants breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PHI/PII;

c. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendants adequately and accurately informed Plaintiffs and Class Members that their PHI/PII had been compromised;

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

f. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PHI/PII of Plaintiffs and Class Members; and

g. Whether Class Members are entitled to actual, consequential and/or nominal damages and/or injunctive relief as a result of Defendants' wrongful conduct.

FIRST CLAIM
NEGLIGENCE
(On Behalf of All Plaintiffs and the Nationwide Class)

156. Each and every allegation of the preceding paragraphs is incorporated in this Claim with the same force and effect as though fully set forth herein.

157. Plaintiffs and the Class entrusted Defendants with their PHI/PII.

158. Plaintiffs and the Class entrusted their PHI/PII to Defendants on the premise and with the understanding that Defendants would safeguard their information, use their PHI/PII only for purposes that would benefit Plaintiffs and the Class and/or not disclose their PHI/PII to unauthorized third parties.

159. Defendants had full knowledge of the sensitivity of the PHI/PII and the types of harm that Plaintiffs and the Class could and would suffer if the PHI/PII was wrongfully disclosed.

160. Defendants knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PHI/PII of Plaintiffs and the Class involved an unreasonable risk of harm to Plaintiffs and the Class, even if the harm occurred through the criminal acts of a third party.

161. Defendants 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. This duty included, among other things, designing, maintaining, and testing Defendants' security protocols to ensure that the PHI/PII of Plaintiffs and the Class in Defendants' possession was adequately secured and protected.

162. Defendants also had a duty to exercise appropriate clearinghouse practices to remove PHI/PII they were no longer required to retain pursuant to various laws and regulations.

163. Defendants also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PHI/PII of Plaintiffs and the Class.

164. Defendants' duty to use reasonable security measures arose as a result of the

special relationship that existed between Defendants and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class entrusted Defendants with their PHI/PII, a necessary part of obtaining services from Defendants.

165. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiffs or the Class.

166. A breach of security, unauthorized access and the resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

167. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the PHI/PII of Plaintiffs and the Class, the critical importance of providing adequate security of that PHI/PII and the necessity for encrypting PHI/PII stored on Defendants' systems.

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

169. Plaintiffs and the Class had no ability to protect their PHI/PII that was in, and possibly remains in, Defendants' possession.

170. Defendants were in a position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

171. Defendants bore and continue to bear a duty to adequately disclose that the PHI/PII of Plaintiffs and the Class within Defendants' possession might have been compromised, how it was compromised and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate and repair any identity theft and/or the fraudulent use of their PHI/PII by third parties.

172. Defendants bore a duty to employ proper procedures to prevent the unauthorized dissemination of the PHI/PII of Plaintiffs and the Class.

173. Defendants have admitted that the PHI/PII of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

174. Defendants, through their actions and/or omissions, unlawfully breached their duties to Plaintiffs and the Class by failing to implement industry protocols and exercise

reasonable care in protecting and safeguarding the PHI/PII of Plaintiffs and the Class during the time the PHI/PII was within Defendants' possession or control.

175. Defendants improperly and inadequately safeguarded the PHI/PII of Plaintiffs and the Class in contravention of standard industry rules, regulations, and practices at the time of the Data Breach.

176. Defendants failed to heed industry warnings and alerts to provide adequate safeguards to protect the PHI/PII of Plaintiffs and the Class in the face of increased risk of theft.

177. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiffs and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of PHI/PII.

178. Defendants breached their duty to exercise appropriate clearinghouse practices by failing to remove PHI/PII they were no longer required to retain pursuant to various laws and regulations.

179. Defendants, through their actions and/or omissions, unlawfully breached their duty to adequately and timely disclose to Plaintiffs and the Class the existence and scope of the Data Breach.

180. But for Defendants' wrongful and negligent breach of duties owed to Plaintiffs and the Class, the PHI/PII of Plaintiffs and the Class would not have been compromised.

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

182. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect PHI/PII. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

183. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PHI/PII and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PHI/PII they obtained and stored, and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

184. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

185. Plaintiffs and the Class are within the class of persons that the FTC Act was intended to protect.

186. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiffs and the Class have suffered and will suffer injury, including, but not limited to: (i) actual identity theft, (ii) the loss of the opportunity to control how their PHI/PII is used, (iii) the compromise, publication, and/or theft of their PHI/PII, (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud and/or unauthorized use of their PHI/PII, (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and continuing consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft, (vi) costs associated with placing freezes on credit reports, (vii) the continued risk to their PHI/PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PHI/PII of Plaintiffs and the Class, and (viii) present and continuing costs in terms of time, effort and money that has been and will be expended to prevent, detect, contest and repair the impact of the PHI/PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Class.

187. As a direct and proximate result of Defendant' negligence and negligence *per se*, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

188. Additionally, as a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their PHI/PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PHI/PII in their continued possession.

189. As a direct and proximate result of Defendants' negligence and negligence *per se*, Plaintiffs and the Class are entitled to recover actual, consequential, and nominal damages.

SECOND CLAIM
BREACH OF IMPLIED CONTRACT
(On behalf of all Plaintiffs and the Nationwide Class)

190. Each and every allegation of the preceding paragraphs is incorporated in this Claim with the same force and effect as though fully set forth herein.

191. Through their course of conduct, Defendants, Plaintiffs and Class Members

entered into implied contracts for Defendants to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' Private Information.

192. Defendants solicited, invited and required Plaintiffs and Class Members to provide their Private Information as part of Defendants' regular business practices. Plaintiffs and Class Members accepted Defendants' offers by, in part, providing their Private Information to Defendants.

193. As a condition of being direct customers and/or employees of Defendants, Plaintiffs and Class Members provided and entrusted their Private Information to Defendants. In so doing, Plaintiffs and Class Members entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such non-public information, to keep such information secure and confidential and to timely and accurately notify Plaintiffs and Class Members if Defendants' data had been breached and compromised or stolen.

194. A meeting of the minds occurred when Plaintiffs and Class Members agreed to, and did, provide their Private Information to Defendants, in exchange for, amongst other things, the protection of their Private Information.

195. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendants.

196. Defendants breached the implied contracts it made with Plaintiffs and Class Members by failing to safeguard and protect their Private Information and by failing to provide timely and accurate notice to them that their Private Information was compromised as a result of the Data Breach.

197. As a direct and proximate result of Defendants' above-described breach of implied contract, Plaintiffs and Class Members have suffered and will continue to suffer (i) ongoing, imminent and impending threat of identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm, (ii) actual identity theft crimes, fraud and abuse, resulting in monetary loss and economic harm, (iii) loss of the confidentiality of the stolen confidential data, (iv) the illegal sale of the compromised data on the dark web, (v) lost work time, and (f) other economic and noneconomic harm.

THIRD CLAIM
INVASION OF PRIVACY
(On Behalf of All Plaintiffs and the Nationwide Class)

198. Each and every allegation of the preceding paragraphs is incorporated in this Claim with the same force and effect as though fully set forth herein.

199. Plaintiffs and Class Members had a legitimate expectation of privacy regarding their PHI/PII and were, accordingly, entitled to the protection of this information against

disclosure to unauthorized third parties.

200. Defendants owed a duty to Plaintiffs and Class Members to keep their PHI/PII confidential.

201. The unauthorized disclosure and/or acquisition (i.e., theft) by a third party of Plaintiffs' and Class Members' PHI/PII is highly offensive to a reasonable person.

202. Defendants' reckless and negligent failure to protect Plaintiffs' and Class Members' PHI/PII constituted a reckless and/or intentional intrusion into Plaintiffs' and the Class Members' interests in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that is highly offensive to a reasonable person.

203. Defendants' failure to protect Plaintiffs' and Class Members' PHI/PII acted with a knowing state of mind when they permitted the Data Breach because they knew their information security practices were inadequate.

204. Defendants' failure to protect Plaintiffs' and Class Members' PHI/PII resulted in the public disclosure of not less than 16 GB of Plaintiffs' and Class Members' PHI/PII on the Dark Web, such disclosure was of a kind that is highly offensive to a reasonable person, the facts disclosed were not of legitimate concern to the public, and Defendants acted with reckless disregard of the private nature of the facts disclosed.

205. Defendants knowingly did not notify Plaintiffs and Class Members in a timely fashion about the Data Breach.

206. Because Defendants failed to properly safeguard Plaintiffs' and Class Members' PHI/PII, Defendants knew their inadequate cybersecurity practices would or would likely cause injury to Plaintiffs and the Class.

207. As a proximate result of Defendants' acts and omissions, the private and sensitive PHI/PII of Plaintiffs and Class Members was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages.

208. Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their PHI/PII is still maintained by Defendants using inadequate cybersecurity system and policies.

209. Plaintiffs and Class Members have no adequate remedy at law for the injuries relating to Defendants' continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendants' inability to safeguard the PHI/PII of Plaintiffs and the Class.

210. Plaintiffs, on behalf of themselves and Class Members, seek injunctive relief to enjoin Defendants from further intruding into the privacy and confidentiality of Plaintiffs' and Class Members' PHI/PII.

211. Plaintiffs, on behalf of themselves and Class Members, seek compensatory damages for Defendants' invasion of privacy, which includes the value of the privacy interest invaded by Defendants, the costs of future monitoring of their credit histories for identity theft and fraud, plus prejudgment interest and costs.

FOURTH CLAIM
UNJUST ENRICHMENT
(On behalf of All Plaintiffs and the Nationwide Class)

212. Each and every allegation of the preceding paragraphs is incorporated in this Claim with the same force and effect as though fully set forth herein.

213. Plaintiffs and Class Members conferred a monetary benefit on Defendants, by providing Defendants with their valuable PHI/PII.

214. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PHI/PII.

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

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

217. Defendants acquired a monetary benefit and the underlying PHI/PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

218. If Plaintiffs and Class Members knew that Defendants had not secured their PHI/PII, they would not have agreed to provide their PHI/PII to Defendant.

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

220. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class

Members have suffered and will suffer injury, including, but not limited to: (i) actual identity theft, (ii) the loss of the opportunity how their PHI/PII is used, (iii) the compromise, publication and/or theft of their PHI/PII, (iv) out-of-pocket expenses associated with the prevention, detection and recovery from identity theft and/or unauthorized use of their PHI/PII, (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest and recover from identity theft, (vi) the continued risk to their PHI/PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect PHI/PII in their continued possession, and (vii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the impact of the PHI/PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

221. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

222. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that Defendants unjustly received.

FIFTH CLAIM
DECLARATORY JUDGMENT
(On Behalf of All Plaintiffs and the Nationwide Class)

223. Each and every allegation of the preceding paragraphs is incorporated in this Claim with the same force and effect as though fully set forth herein.

224. Under CO Rev. Stat. § 13-51-106, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief.

225. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective common law and other duties to reasonably safeguard their customers' PHI/PII and with regard to whether Defendants are currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their PII/PHI. Plaintiffs allege that Defendants' data security measures remain inadequate. Defendants deny these allegations. Furthermore, Plaintiffs and Class Members continue to suffer injury as a result of the compromise of their PHI/PII and remain at imminent risk that further compromises of their PHI/PII will occur in the future.

226. Pursuant to its authority under CO Rev. Stat. § 13-51-106, this Court should enter a judgment declaring, among other things, the following:

a. Defendants continue to owe a legal duty to secure consumers' PHI/PII (including Personal Information) and to timely notify consumers of a data breach under the common law and Section 5 of the FTC Act;

b. Defendants continue to breach this legal duty by failing to employ reasonable measures to secure consumers' PHI/PII.

227. The Court also should issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with law and industry standards to protect consumers' PHI/PII.

228. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach affecting Defendants. The risk of another such breach is real, immediate, and substantial. If another breach affecting Defendants occurs, Plaintiffs and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and/or quantifiable, and because they will be forced to bring multiple lawsuits to rectify the same conduct.

229. The hardship to Plaintiffs and Class Members if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. Among other things, if another large scale data breach affecting Defendants occurs, Plaintiffs and Class Members will likely be subjected to substantial identify theft and other damage. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures anyway.

230. Imposition of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach affecting Defendants, thus eliminating the additional injuries that would result to Plaintiffs and numerous of consumers whose confidential and valuable information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendants, and that the Court grant the following:

1. That the Court declare, adjudge and decree that this action is a proper class action and certify each of the proposed Class pursuant to Colorado Rules of Civil Procedure Rule 23, including appointment of Representative Plaintiffs' counsel as Class Counsel;

2. For an award of damages, including, but not limited to, actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

3. That the Court enjoin Defendants, ordering them to cease and desist from unlawful activities;

4. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and Class Members;

5. For injunctive relief requested by Representative Plaintiffs, including, but Injunctive relief, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including, but not limited to, an Order:

a. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

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

c. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

d. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PHI/PII of Plaintiffs and Class Members;

e. prohibiting Defendants from maintaining the PHI/PII of Plaintiffs and Class Members on a cloud-based database;

f. requiring Defendants 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 Defendants' systems on a periodic basis and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

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

h. requiring Defendants to audit, test and train their security personnel regarding any new or modified procedures;

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

j. requiring Defendants to conduct regular database scanning and securing checks;

k. requiring Defendants 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 Plaintiffs and Class Members;

l. requiring Defendants 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;

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

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

o. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their PHI/PII to third parties, as well as the steps affected individuals must take to protect themselves;

p. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' 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 Defendants' 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;

6. Penalties, and treble and other damages, as permitted by law;

7. An award of attorneys' fees, costs and litigation expenses, as permitted by law;

8. Prejudgment interest on all amounts awarded, at the prevailing legal rate; and

9. For all other Orders, findings and determinations identified and sought in this Complaint.

DEMAND FOR JURY TRIAL

Plaintiffs, individually, and on behalf of the Nationwide Class, hereby demand a trial by jury for all issues so triable.

Date: February 24, 2025

Respectfully submitted,

/s/ Reid Elkus

Reid Elkus (CO. BAR #32516)
ELKUS & SISSON, P.C.
7100 E Belleview Avenue, Suite 101
Greenwood Village, CO 80111
Tel: (303) 567-7981
relkus@elkusandsisson.com

Joseph M. Lyon* (OH BAR #76050)
THE LYON FIRM
2754 Erie Ave.
Cincinnati, OH 45208
Tel: (513) 381-2333
jlyon@thelyonfirm.com

Respectfully submitted,

/s/ Scott Edward Cole

Scott Edward Cole* (CA BAR #160744)
Mark T. Freeman* (CA BAR #293721)
COLE & VAN NOTE
555 12th Street, Suite 2100
Oakland, California 94607
Tel: (510) 891-9800
sec@colevannote.com
mtf@colevannote.com

Amber L. Schubert* (CA BAR #278696)
SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St., Suite 200
San Francisco, California 94123
Tel: (415) 788-4220
aschubert@sjk.law

*Pro Hac Vice forthcoming