UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

LELAND WOOTEN, JR., Individually and on Behalf of All Others Similarly Situated, Plaintiff, v. GREYLOCK MCKINNON ASSOCIATES, INC., Defendant.	Case No.: _____ **CLASS ACTION COMPLAINT** **Jury Trial Demanded**

Upon personal knowledge as to his own acts, and based upon his investigation, the investigation of counsel, and information and belief as to all other matters, Plaintiff Leland Wooten, Jr., on behalf of himself and all others similarly situated, alleges as follows:

SUMMARY OF THE ACTION

1. Plaintiff brings this class action against Greylock McKinnon Associates, Inc. ("Greylock" or "Defendant") for its failure to adequately secure and safeguard his and at least 341,650 total individuals' personally identifying information ("PII") and protected health information ("PHI"), including names, mailing addresses, phone numbers, dates of birth, Social Security or Taxpayer Identification numbers, driver's license or state identification numbers, Medicare Beneficiary Identifiers (MBIs) or Health Insurance Claim Numbers (HICNs), healthcare provider and prescription information, health insurance claims and policy and subscriber information, health benefits and enrollment information, and medical records and medical histories, including medical conditions, among other potentially sensitive, private, and confidential data.

2. Greylock is a Massachusetts-based consulting firm that provides expert economic analysis and litigation support services in civil litigation matters. Its clients include legal, business, and government stakeholders, and at various times relevant here, the U.S. Department of Justice (the "DOJ"). In addition to Greylock's Boston, Massachusetts headquarters, Defendant maintains offices in Washington, D.C. and Hanover, New Hampshire.

3. In the ordinary course of providing consulting and other services to its clients and other entities and persons, Greylock received PII and PHI from at least hundreds of thousands of persons, including from Plaintiff and Class Members (defined herein). In turn, Greylock comes into the possession of, and maintains extensive files containing, the PII and PHI of its clients and other third-party persons (including Medicare beneficiaries), and owes these individuals an affirmative duty to adequately protect and safeguard this private information against theft and misuse. Despite such duties created by statute, regulation, common law, and equity, at all relevant times, Greylock utilized deficient data security practices, thereby allowing hundreds of thousands of persons' sensitive and private data to fall into the hands of strangers and cyberthieves.

4. On May 30, 2023, Greylock lost control over this highly sensitive and confidential PII and PHI of Plaintiff and the Class Members in a massive and preventable data breach apparently perpetrated by cybercriminals (the "Data Breach"). According to Greylock, on May 30, 2023, it "detected unusual activity on our internal network" and then "promptly took steps to mitigate the incident."[1] Greylock has not specifically explained what, if anything, it did to cut off the bad actors' access to its systems, but claims to have "consulted with third-party

[1] *Sample Notice of a Security Incident*, GREYLOCK MCKINNON ASSOCIATES, INC. (Feb. 23, 2024), Exhibit 1.

cybersecurity specialists to assist with [its] response to the incident."[2] Some iterations of Greylock's Data Breach notices informed individuals that their personal information "may have been affected" (February 23, 2024) or "was likely affected" (April 8, 2024),[3] without explaining whether any of Greylock's files were actually stolen, copied, or downloaded. However, additional notices issued by the DOJ—with whom Greylock contracted for various services—provided additional clarity regarding critical information missing from Greylock's Data Breach notices. For example, the DOJ revealed for the first time that the "incident" was a ransomware attack, that "several" of Greylock's systems were affected, and that copies of "several" of Greylock's files were actually "obtained" and "exfiltrated."[4] Greylock has not disclosed whether it paid any ransom in connection with the cyberattack or for how long cybercriminals had unfettered access to Plaintiff's and the Class's highly private information.

5. The Data Breach was directly and proximately caused by Greylock's failure to implement and maintain reasonable and industry-standard data security practices necessary to protect its systems from a foreseeable and preventable cyberattack. Through this wrongful conduct, the sensitive PII and PHI of more than 340,000 individuals is now in the hands of cybercriminals, who target this sensitive data for its value to identity thieves. Plaintiff and Class Members are now at a significantly increased and impending risk of fraud, identity theft, and similar forms of criminal mischief—risks which may last the rest of their lives. Consequently, Plaintiff and Class Members must devote substantially more time, money, and energy to protect

[2] *See id.*

[3] *Sample Notice of Data Breach*, GREYLOCK MCKINNON ASSOCIATES, INC. (Apr. 8, 2024), Exhibit 2.

[4] *Notice of Breach*, U.S. DEPARTMENT OF JUSTICE (Apr. 5, 2024), Exhibit 3.

themselves, to the extent possible, from these crimes. Moreover, Plaintiff and Class Members have lost the inherent value of their private data.

6. By aggregating information obtained from the Data Breach with other sources or other methods, criminals can assemble a full dossier of private information on an individual to facilitate a wide variety of frauds, thefts, and scams. Criminals can and do use victims' names and other personal information to open new financial accounts, incur credit and bank charges on existing accounts, obtain government benefits and identifications, fabricate identities, and file fraudulent tax returns well before the person whose PII was stolen becomes aware of it. Any one of these instances of identity theft can have devastating consequences for the victim, causing years of often irreversible damage to their credit scores, financial stability, and personal security. Likewise, the exfiltration of protected health information puts Plaintiff and the Class Members at a present and continuing risk of medical identity theft, which poses an even more critical threat to victims because such fraud could lead to loss of access to necessary healthcare through misuse of paid-for insurance benefits or by incurring substantial medical debt.

7. Despite learning of the ransomware Data Breach on May 30, 2023, Greylock only began notifying some impacted persons ***almost nine months later***, around February 23, 2024. Even with this long lag, Greylock still had little grasp on the true scope of the cyberattack. In a public filing with the Maine Attorney General's Office, Greylock indicated that the Data Breach affected just 5,465 total persons.[5] The bulk of the Data Breach notices issued about six weeks later, around April 5, 2024—***more than ten months*** after Greylock learned of the Data Breach. In a subsequent Maine Attorney General's Office filing, Greylock disclosed that the Data Breach

[5] Office of the Maine Attorney General, Data Breach Notifications, *available at* https://apps.web.maine.gov/online/aeviewer/ME/40/c8e05b1c-ddad-475b-b643-39e62eaefab7.shtml.

was ***more than sixty-times larger than previously revealed***, actually affecting 341,650 persons.[6] This extreme delay exacerbated the damages and risks to Plaintiff and Class Members, and violated various state data breach notification statutes and rules promulgated under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The Data Breach notice letters to victims also obscure the true nature of the Greylock cyberattack and threat it posed—failing to adequately inform Plaintiff and Class Members how many people were impacted, how an unauthorized third party accessed Greylock's systems, copied its files, and the root cause of the Data Breach, whether Greylock paid the demanded ransom, what specific PII and PHI was stolen for each affected person, whether the exfiltrated information was encrypted or anonymized, why it took so long to notify victims, whether Greylock or law enforcement have apprehended or even identified the hackers who accessed Greylock's systems, or what specific remedial steps Greylock has taken to safeguard PII and PHI within its systems and networks (or otherwise purge unnecessary information) and to prevent further cyberattacks going forward. Without these critical details, Plaintiff and Class Members cannot meaningfully mitigate the resulting effects of the Greylock Data Breach.

8. Plaintiff Wooten, Jr. is a Data Breach victim and first received a notification of the Data Breach from the DOJ (not Greylock) by letter dated April 5, 2024.

9. Plaintiff, on behalf of himself and all others similarly situated, herein alleges claims for negligence, negligence *per se*, invasion of privacy, breach of third-party beneficiary contract, unjust enrichment or quasi-contract, and declaratory and injunctive relief. Plaintiff, on behalf of himself and the Class, seeks: (i) actual damages, economic damages, statutory damages,

[6] Office of the Maine Attorney General, Data Breach Notifications, *available at* https://apps.web.maine.gov/online/aeviewer/ME/40/865575ae-973b-4430-a06c-d780da040c74.shtml.

and nominal damages; (ii) punitive damages; (iii) fees and costs of litigation; (iv) injunctive relief, including the adoption of reasonably sufficient practices to safeguard PII and PHI in Defendant's custody, care, and control in order to prevent incidents like the Data Breach from recurring in the future and for Greylock to provide long-term, comprehensive identity theft protective services to Plaintiff and Class Members; and (v) such other relief as the Court deems just and proper.

PARTIES

A. Plaintiff

10. Plaintiff Leland Wooten, Jr. is a resident and citizen of Florida, residing in Cocoa, Florida.

B. Defendant

11. Defendant Greylock McKinnon Associates, Inc. is a corporation organized under the laws of the State of Massachusetts. Greylock maintains its corporate headquarters and principal place of business at 75 Park Plaza, Fourth Floor, Boston, Massachusetts 02116.

JURISDICTION AND VENUE

12. This Court has original jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because at least member of the putative Class, as defined below, is a citizen of a state other than that of Defendant, there are more than 100 putative Class Members, and the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs.

13. This Court has personal jurisdiction over Greylock because Defendant is a Massachusetts corporation, maintains its principal place of business in Boston, Massachusetts,

regularly conducts business in Massachusetts, and has sufficient minimum contacts in Massachusetts, such as to not offend traditional notions of fair play and substantial justice.

14. Venue is proper in this District under 28 U.S.C. §§ 1391(b), (c), and (d) because Greylock is a Massachusetts corporation (and thus resides in this District), is headquartered in Massachusetts, and a substantial part of the conduct giving rise to Plaintiff's claims and resulting harms occurred in this District, including Defendant collecting or storing the PII and PHI of Plaintiff and the putative Class Members.

FACTUAL BACKGROUND

A. Greylock Collects, Stores, and Maintains Huge Amounts of Personally Identifiable Information and Protected Health Information.

15. Greylock states that it "provides expert economic analysis and litigation support to a diverse group of domestic and international clients in the legal profession, the business community, and government agencies."[7] It "works with domestic and international corporations ranging from Fortune 100 companies to small regional companies and state and federal governmental agencies."[8] Greylock purports to "respect the value that many of [its] clients place

[7] GREYLOCK MCKINNON ASSOCIATES, https://www.gma-us.com/ (last visited May 27, 2024).

[8] *Id.*

on confidentiality."[9] The company employs over thirty professionals[10] and generates approximately $5 million in annual revenue.[11]

16. To obtain Greylock's consulting and litigation services, its clients provided Defendant with a wide array of highly sensitive information, including health information. In doing so, Greylock made explicit and implicit promises and representations to its clients that provided such data, including entities like the DOJ, that Defendant would keep this information safe and confidential. Plaintiff's and Class Members' PII and PHI was thus provided to Greylock by Greylock's clients with the reasonable expectation and on the mutual understanding that Greylock would comply with its obligations to keep such information confidential and secure from unauthorized access. Greylock derived a substantial economic benefit from collecting Plaintiff's and Class Members' PII and PHI. Without the required submission of this private information, Greylock could not performed the services it provides to its clients.

17. Given the scope of its services and wide client base, Greylock's networks, files, and servers maintain, in total, at least several hundreds of thousands of persons' most private information.

18. Despite its duties and obligations to adopt and maintain reasonable cybersecurity measures, Greylock failed to adequately secure and safeguard its systems and networks from a

[9] *See id.*

[10] Our Professionals, GREYLOCK MCKINNON ASSOCIATES, https://www.gma-us.com/professionals/ (last visited May 27, 2024).

[11] Greylock McKinnon Associates Information, ROCKETREACH, https://rocketreach.co/greylock-mckinnon-associates-profile_b7e6c2f9c07c2c34 (last visited May 20, 2024).

foreseeable and preventable cyberattack. This conduct proximately resulted in the Data Breach and significant harm to Plaintiff and the Class.

B. The Data Breach Exposed Valuable PII and PHI

19. Greylock collected and maintained Plaintiff's and the Class's PII and PHI in its computer systems, servers, and networks. In accepting, collecting, and maintaining Plaintiff's and the Class's PII and PHI, Greylock agreed that it would protect and safeguard that data by complying with state and federal laws and regulations and applicable industry standards. Greylock was in possession of Plaintiff's and the Class's PII and PHI before, during, and, at least for some period, after the Data Breach.

20. According to Greylock's Data Breach letters, on May 30, 2023, it "detected unusual activity on [its] internal network" and "was the victim of a sophisticated cyberattack."[12] Later iterations of the Data Breach letters issued by the DOJ (a Greylock client) provide additional clarity about the Data Breach, revealing that the May 30, 2023 incident was a "ransomware attack" targeting Greylock. Neither of Greylock's February 23, 2024 or subsequent April 8, 2024 Data Breach letters (nor the DOJ's April 5, 2024 letters) disclose whether Greylock paid any ransom in connection with the cyberattack or for how long cybercriminals had unfettered access to Plaintiff's and the Class's highly private information on Greylock's networks. The DOJ's Data Breach letters confirm that PII and PHI was actually stolen by the hacker during the Data Breach, explaining that the cybersecurity incident "resulted in the exposure and exfiltration of several files in [Greylock]'s possession."[13]

[12] Exhibit 1.

[13] *See* Exhibit 3.

21. Around February 23, 2024—***more than eight months after it learned of the ransomware attack***—Greylock reported the Data Breach to various governmental agencies and attorneys general and began sending Data Breach letter to some affected persons. Therein, Greylock stated that it took until February 5, 2024, following "an extensive forensic review" to determine which individuals' data had been stolen. Greylock offers no meaningful explanation for this extreme delay. At the time, Greylock represented that only 5,465 individuals' PII and PHI were compromised.

22. Six weeks later, around April 5, 2024—***more than ten months after the Data Breach***—Greylock made a subsequent filing with the Maine Attorney General's Office attaching a follow-on Data Breach letter. As of April 5, 2024, Greylock reported to the Maine Attorney General's Office that the total number of persons affected by the May 30, 2023 Data Breach had ballooned to 341,650. In the new letter, Greylock explained that it had obtained individuals' PII and PHI from the DOJ in connection with a civil litigation matter. Again, Greylock offers no meaningful explanation for its extreme delay in notifying affected persons or why it grossly underreported in February 2024 the number of persons impacted by the Data Breach.

23. Despite Greylock's duties to safeguard sensitive and private information, Greylock failed to follow industry-standard practices in securing Plaintiff's and the Class Members' PII and PHI, as evidenced by the Data Breach.

24. In response to the Data Breach, Greylock contends that it "promptly took steps to mitigate the incident."[14] Greylock does not explain what, if any, additional cybersecurity safeguards it subsequently implemented, but any such changes it did take clearly should have been in place and fully operational *before* the Data Breach. While the Data Breach letters state

[14] *See* Exhibit 1.

that it "deleted DOJ data from its systems,"[15] Greylock has not yet affirmed that all PII and PHI of Plaintiff and the Class has been purged from its files, servers, networks, and systems. Additionally, although Greylock indicated that it notified law enforcement of the Data Breach, the Data Breach letters do not state whether the criminals responsible for the Data Breach have been identified or apprehended.

25. Greylock's Data Breach letters reveal that a treasure trove of information from Plaintiff and the Class was stolen in the cyberattack, including, at least: names, mailing addresses, phone numbers, dates of birth, Social Security or Taxpayer Identification numbers, driver's license or state identification numbers, Medicare Beneficiary Identifiers (MBIs) or Health Insurance Claim Numbers (HICNs), healthcare provider and prescription information, health insurance claims and policy and subscriber information, health benefits and enrollment information, and medical records and medical histories, including medical conditions.

26. Through the Data Breach letters, Greylock also recognized the actual imminent harm and injury that flowed from the Data Breach, saying "[W]e recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies."[16] Greylock offered certain Class Members only either one year (February 2024 letters) or two years (April 2024 letters) of complimentary identity monitoring services through its hand-picked vendors, Experian and TransUnion, respectively. The DOJ offered Plaintiff Wooten, Jr. one year of credit monitoring through Sontiq, but he has not received any offer of comparable services from Greylock itself.

[15] Exhibit 2; Exhibit 3.

[16] *Id.*

27. These offers do not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the Data Breach involves PII that is difficult or even impossible to change, such as Social Security numbers and dates of birth. Further, the Data Breach exposed nonpublic, highly private information, including PHI, which is disturbing harm in of itself. Even with complimentary short-term identity monitoring services, the risk of identity theft and unauthorized use of Plaintiff's and Class Members' PII and PHI is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

C. Consulting Firms and Other Businesses Warehousing Large Amounts of Valuable PII and PHI Are Increasingly Susceptible to Data Breaches, Giving Greylock Ample Notice That It Was a Likely Cyberattack Target

28. At all relevant times, Greylock knew, or should have known, that the PII and PHI it was entrusted with was a prime target for malicious actors. Defendant knew this given the unique type and the significant volume of data on its networks, servers, and systems, comprising individuals' detailed and confidential personal information and, thus, the significant number of individuals who the exposure of the unencrypted data would harm.

29. As custodian of Plaintiff's and Class Members' PII and PHI, Greylock knew or should have known the importance of protecting their PII and PHI, and of the foreseeable consequences and harms to such persons if any data breach occurred.

30. Ransomware "is a type of malicious software (malware) that threatens to publish or blocks access to data or a computer system, usually by encrypting it, until the victim pays a ransom fee to the attacker. In many cases, the ransom demand comes with a deadline. If the victim doesn't pay in time, the data is gone forever or the ransom increases."[17] Additionally,

[17] *What is Ransomware?*, PROOFPOINT, https://www.proofpoint.com/us/threat-reference/ransomware (last visited May 27, 2024).

ransomware groups regularly sell stolen data in cybercriminal forums and dark web marketplaces for additional revenue,[18] causing the compromised information to fall into the hands of countless other persons. Companies should thus treat ransomware attacks as any other data breach incident.

31. For many years and prompted by the September 2017 data breach of one of the "Big Four" consulting firms (Deloitte), Greylock was or should have been on notice of the following trend: "consulting firms are coming into the cross-hairs of cyber villains."[19] In its June 2018 report, cybersecurity firm PreVeil declared that cybercriminals "have woken up and realized they stand to profit from relieving consulting firms of their data."[20] PreVeil advised that, "Whether you're 30-person boutique consulting shop or 10,000+ person firm, your firm's email and digital file servers represent an extremely high value target to cyber criminals."[21] PreVeil warned that "it is not a question of *'if'*, but rather *'when',* advanced persistent attackers will find a way into your network," urging consulting firms both "large and small to better protect the sensitive client files and emails they're entrusted with."[22] In the wake of Deloitte's 2017 data breach and other cybersecurity incidents affecting PwC and Booze Allen, PreVeil told consulting firms that "cybersecurity is your business whether you like it or not."[23]

32. Defendant's security obligations were also especially important due to the substantial increase of cyberattacks and data breaches in recent years, particularly those targeting

---

[18] *Ransomware: The Data Exfiltration and Double Extortion Trends*, CENTER FOR INTERNET SECURITY, https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends (last visited May 27, 2024).

[19] *Consulting Firms Under Attack: How to Protect You and Your Clients*, PREVEIL (June 2018), https://www.preveil.com/wp-content/uploads/2019/10/Consulting-blog-June-2018.pdf.

[20] *Id.*

[21] *Id.*

[22] *Id.*

[23] *Id.*

businesses and other organizations like Defendant, which store and maintain large volumes of PII and PHI. These largescale cyberattacks are increasingly common and well-publicized. In 2023, a total of 725 largescale cyberattacks targeted hospitals, health systems, and healthcare records, affecting more than 133 million people—making 2023 the "worst-ever year for breached healthcare records."[24] Additionally, professional services companies were the third-most targeted industry for data breaches in 2023, comprising about 12% of all data breaches.[25] On average, the consulting industry faced 837 cyberattacks every week in 2023.[26] With the surging number of such attacks targeting companies in or adjacent to the healthcare sector, Greylock knew or should have known that it was at high risk of cyberattack and should have taken additional and stronger precautions and preemptive measures.

D. Greylock Breached Its Duties to Plaintiff and the Class Members, and Failed to Comply with Regulatory Requirements and Industry Practices.

33. Because Defendant was entrusted with PII and PHI at all times herein relevant, Greylock owed to Plaintiff and the Class a duty to exercise commercially reasonable methods and care in handling, using, maintaining, storing, and safeguarding the PII and PHI in its care, control, and custody, including by implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that occurred, and to promptly detect and thwart attempts at unauthorized access to its networks and

[24] Steve Alder, *Security Breaches in Healthcare in 2023*, THE HIPAA JOURNAL (Jan. 31, 2024), https://www.hipaajournal.com/security-breaches-in-healthcare/.

[25] David White, *Data Breach Outlook: Finance Surpasses Healthcare as Most Breached Industry in 2023*, KROLL (Feb. 7, 2024), https://www.kroll.com/en/insights/publications/cyber/data-breach-outlook-2024.

[26] *Check Point Research: 2023 – The year of Mega Ransomware attacks with unprecedented impact on global organizations*, Check Point (Jan. 16, 2024), https://blog.checkpoint.com/research/check-point-research-2023-the-year-of-mega-ransomware-attacks-with-unprecedented-impact-on-global-organizations/.

systems. Defendant also owed a duty to safeguard PII and PHI because it was on notice that it was handling highly valuable data and knew there was a significant risk it would be targeted by cybercriminals. Furthermore, Greylock knew of the extensive, foreseeable harm that would ensue for the victims of a data breach, and therefore also owed a duty to reasonably safeguard that information.

34. Security standards commonly accepted among companies like Greylock that store PII and PHI include, without limitation:

i. Maintaining a secure firewall configuration;

ii. Monitoring for suspicious or irregular traffic to servers or networks;

iii. Monitoring for suspicious credentials used to access servers or networks;

iv. Monitoring for suspicious or irregular activity by known users;

v. Monitoring for suspicious or unknown users;

vi. Monitoring for suspicious or irregular server requests;

vii. Monitoring for server requests for PII or PHI;

viii. Monitoring for server requests from virtual private networks (VPNs); and

ix. Monitoring for server requests for Tor exit nodes.

35. Regarding ransomware attacks like that experienced by Greylock, the Federal Bureau of Investigation ("FBI") advises that "Proactive Prevention is the Best Defense."[27] To protect against these types of cyberattacks, Greylock should have adopted the following measures, as recommended by the U.S. Government:

[27] How to Protect Your Networks from RANSOMWARE, FEDERAL BUREAU OF INVESTIGATION, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

i. 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;

ii. Enable strong spam filers 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;

iii. Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users;

iv. Configure firewalls to block access to known malicious IP addresses;

v. Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system;

vi. Set anti-virus and anti-malware programs to conduct regular scans automatically;

vii. 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;

viii. 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;

ix. Disable macro scripts form office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications;

x. 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;

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

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

xiii. Execute operating system environments or specific programs in a virtualized environment; and

xiv. Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[28]

36. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for cybersecurity[29] and protection of PII which includes basic security standards applicable to all types of businesses.[30]

37. The FTC recommends that businesses:

i. Identify all connections to the computers where sensitive information is stored.

ii. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

---

[28] *Id.*

[29] Start with Security: A Guide for Business, FTC (June 2015), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[30] Protecting Personal Information: A Guide for Business, FTC (Oct. 2016), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

iii. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

iv. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

v. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hacker attacks.

vi. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

vii. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

viii. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

ix. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business's network, the transmission should be investigated to make sure it is authorized.

38. As described further below, Defendant owed a duty to safeguard PII and PHI under several statutes, including the Federal Trade Commission Act, 15 U.S.C. § 45 (the "FTC Act") and as a business associate under HIPAA, to ensure that all information it received, maintained, and stored was secure. These statutes were enacted to protect Plaintiff and the Class Members from the type of conduct in which Defendant engaged, and the resulting harms Defendant proximately caused Plaintiff and the Class Members.

39. Under the FTC Act, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard the PII and PHI of Plaintiff and Class Members. Under HIPAA, 42 U.S.C. §§ 1320d, *et seq.*, and its implementing regulations, 45 C.F.R. §§ 160, *et seq.*, Defendant had a duty to securely store and maintain the PII and PHI of Plaintiff and Class Members which was collected in conjunction with performing consulting services for its clients.

40. Defendant breached its duty to exercise reasonable care in protecting Plaintiff's and Class Members' PII and PHI by failing to implement and maintain adequate data security measures to safeguard Plaintiff's and Class Members' sensitive personal information, failing to encrypt or anonymize PII and PHI within its systems and networks, failing to monitor its systems and networks to promptly identify and thwart suspicious activity, failing to delete and purge PII and PHI no longer necessary for its provision of consulting services to its clients and other entities and persons, allowing unmonitored and unrestricted access to unsecured PII and PHI, and allowing (or failing to prevent) unauthorized access to, and exfiltration of, Plaintiff's and Class

Members' confidential and private information. Additionally, Defendant breached its duty by utilizing outdated and ineffectual data security measures which deviated from standard industry best practices at the time of the Data Breach. Through these actions, Greylock also violated its duties under the FTC Act and HIPAA.

41. Defendant failed to prevent the Data Breach. Had Greylock properly maintained and adequately protected its systems, servers, and networks, the Data Breach would not have occurred.

42. Additionally, the law imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of PII and PHI to Plaintiff and Class Members so that they can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuses of their private information. Greylock further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Class Members. In so doing, Defendant actually and proximately caused and exacerbated the harm from the Data Breach and the injuries-in-fact of Plaintiff and Class Members.

E. The Experiences of Plaintiff Wooten, Jr.

43. Plaintiff Wooten, Jr. received notice of the Data Breach by letter from the DOJ dated April 5, 2024.

44. As a proximate result of the Data Breach, Wooten, Jr. will spend time for the foreseeable future and beyond dealing with its consequences and self-monitoring his accounts and credit reports to monitor potentially suspicious and fraudulent activity. This time will be lost forever and cannot be recaptured.

45. Wooten, Jr. is extremely concerned about his most private and personal medical information being compromised in the Data Breach, the uncertainty surrounding how Greylock

came to possess his information in the first instance, and not knowing who stole his information or for what purpose. This goes beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a data breach victim that the law contemplates and addresses.

46. Wooten, Jr. suffered actual injuries in the form of damages to and diminution in the value of his PII and PHI—a form of intangible property that was entrusted to Greylock, which was compromised in and as a proximate result of the Data Breach.

47. Wooten, Jr. has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from his PII and PHI being obtained by unauthorized third parties and likely cybercriminals.

48. Wooten, Jr. has a continuing interest in ensuring that his PII and PHI, which may remain within Greylock's possession and control, is protected and safeguarded against future data breaches or cybersecurity risks.

49. Defendant deprived Wooten, Jr. of the earliest opportunity to guard himself against the Data Breach's harmful effects by failing to promptly notify him about it. Instead, ***Greylock waited over ten months***, without any meaningful explanation.

F. Plaintiff Wooten, Jr. and the Class Suffered Actual and Impending Injuries Resulting from the Data Breach

50. As a proximate result of Defendant's completely unreasonable security practices, identity thieves now possess the sensitive PII and PHI of Wooten, Jr. and the Class. That information is extraordinarily valuable on the black market and incurs direct costs to Wooten, Jr. and the Class. On the dark web—an underground internet black market—criminals openly buy and sell stolen PII and PHI to create "identity kits" worth up to $2,000 each that can be used to create fake IDs, gain access to bank accounts, social media accounts, and credit cards, file false

insurance claims or tax returns, or rack up other kinds of expenses.[31] And, "[t]he damage to affected [persons] may never be undone."[32]

51. Unlike the simple credit-card breaches at retail merchants, these damages cannot be avoided by canceling and reissuing plastic cards or closing an account. Identity theft is far more pernicious than credit card fraud. Criminals' ability to open entirely new accounts—not simply prey on existing ones—poses far more dangerous problems. Identity thieves can retain the stolen information for years until the controversy has receded because victims may become less vigilant in monitoring their accounts as time passes. Then, at any moment, the thief can take control of a victim's identity, resulting in thousands of dollars in losses and lost productivity. The DOJ reported that in 2021, identity theft victims spent on average about four hours to resolve problems stemming therefrom and that the average financial loss experienced by an identity theft victim was $1,160 per person.[33] Additionally, about 80% of identity theft victims reported some form of emotional distress resulting from the incident.[34]

52. As a consequence of the Data Breach, Plaintiff's and Class Members' credit profiles can be destroyed before they even realize what happened, and they may be unable to legitimately borrow money, obtain credit, or open bank accounts. Plaintiff and Class Members can be deprived of legitimate tax refunds or, worse yet, may face state or federal tax

---

[31] Nick Culbertson, *Increased Cyberattacks on Healthcare Institutions Shows the Need for Greater Cybersecurity*, FORBES (Jun. 7, 2021), https://www.forbes.com/sites/forbestechcouncil/2021/06/07/increased-cyberattacks-on-healthcare-institutions-shows-the-need-for-greater-cybersecurity/?sh=ca928c05650d.

[32] *Id.*

[33] Erika Harrell and Alexandra Thompson, Victims of Identity Theft, 2021, U.S. DEPARTMENT OF JUSTICE, OFFICE OF JUSTICE PROGRAMS, BUREAU OF JUSTICE STATISTICS (Oct. 2023), *available at* https://bjs.ojp.gov/document/vit21.pdf.

[34] *Id.*

investigations due to fraud committed by an identity thief. And even the simple preventive step of adding oneself to a credit-fraud watch list to guard against these consequences substantially impairs Plaintiff's and Class Members' ability to obtain additional credit. In fact, many experts advise victims to place a freeze on all credit accounts, making it impossible to rent a car, get student loans, buy or rent big-ticket items, or complete a major new car or home purchase.

53. Cybercriminals sell health information at a far higher premium than stand-alone PII. This is because health information enables thieves to go beyond traditional identity theft and obtain medical treatments, purchase prescription drugs, submit false bills to insurance companies, or even undergo surgery under a false identity.[35] The shelf life for this information is also much longer—while individuals can update their credit card numbers, they are less likely to change their health insurance information. When medical identity theft occurs, the associated costs to victims can be exorbitant. According to a 2015 study, at least 65% of medical identity theft victims had to "pay an average of $13,500 to resolve the crime."[36]

54. Greylock's Data Breach notices to affected persons do not provide adequate remediation and compensation for its wrongful conduct and actions described herein. Therein, Greylock says that it "sincerely regret[s] any inconvenience or concern this incident may cause"[37] affected individuals, but only offered them, at most, two years of complimentary identity protection service through its hand-picked vendors, Experian and TransUnion.

---

[35] Medical Identity Theft: FAQs for Health Care Providers and Health Plans, FTC, *available at* https://www.ftc.gov/system/files/documents/plain-language/bus75-medical-identity-theft-faq-health-care-health-plan.pdf.

[36] Justin Klawans, *What is medical identity theft and how can you avoid it?*, THE WEEK (Aug. 2, 2023), https://theweek.com/feature/briefing/1025328/medical-identity-theft-how-to-avoid.

[37] Exhibit 1.

CLASS ACTION ALLEGATIONS

55. Pursuant to Federal Rule of Civil Procedure 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiff seeks certification of the following nationwide class (the "Class"):

> All persons residing in the United States whose PII or PHI was compromised in the Data Breach discovered by Greylock on or about May 30, 2023, including all persons who were sent a notice of the Data Breach (and each person a "Class Member").

56. Excluded from the Class are governmental entities, Greylock, any entity in which Greylock has a controlling interest, and Greylock's officers, directors, affiliates, legal representatives, co-conspirators, successors, subsidiaries, and assigns. Also excluded from the Class are any judges, justices, or judicial officers presiding over this matter and the members of their immediate families and judicial staff.

57. This action is brought and may be properly maintained as a class action pursuant to Federal Rule of Civil Procedure 23(b)(2) and 23(b)(3), and satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of these rules.

58. ***Numerosity Under Rule 23(a)(1).*** The Class is so numerous that the individual joinder of all members is impracticable, and the disposition of the claims of all members of the Class in a single action will provide substantial benefits to the parties and the Court. Although the precise number of members of the Class is unknown to Plaintiff at this time, on information and belief, the proposed Class contains at least 341,650 individuals, as reported to the Maine Attorney General. Discovery will reveal, through Greylock's records, the actual number of members of the Class.

59. ***Commonality Under Rule 23(a)(2).*** Common legal and factual questions exist that predominate over any questions affecting only individual Class Members. These common

questions, which do not vary among Class Members, and which may be determined without reference to any Class Member's individual circumstances, include, but are not limited to:

(a) Whether Defendant knew or should have known that its computer systems and networks were vulnerable to unauthorized third-party access or a cyberattack;

(b) Whether Defendant failed to utilize and maintain adequate and reasonable security and preventive measures to ensure that its computer systems and networks were protected;

(c) Whether Defendant failed to take available steps to prevent and stop the Data Breach from occurring;

(d) Whether Defendant owed a legal duty to Plaintiff and Class Members to protect their PII and PHI;

(e) Whether Defendant breached any duty to protect the PII or PHI of Plaintiff and Class Members by failing to exercise due care in protecting their sensitive and private information;

(f) Whether Defendant provided timely, accurate, and sufficient notice of the Data Breach to Plaintiff and the Class Members;

(g) Whether Plaintiff and Class Members have been damaged by the wrongs alleged and are entitled to actual, statutory, or other forms of damages and other monetary relief; and

(h) Whether Plaintiff and Class Members are entitled to injunctive or equitable relief, including restitution.

60. ***Typicality Under Rule 23(a)(3).*** Plaintiff's claims are typical of the claims of the Class. Wooten, Jr., like all proposed members of the Class, had his PII or PHI compromised in the Data Breach. Greylock's uniformly unlawful course of conduct injured Wooten, Jr. and Class

Members in the same wrongful acts and practices. Likewise, Wooten, Jr. and other Class Members must prove the same facts in order to establish the same claims.

61. ***Adequacy of Representation Under Rule 23(a)(4).*** Wooten, Jr. is an adequate representative of the Class because he is a Class Member and his interests do not conflict with the interests of the Class. Wooten, Jr. has retained counsel competent and experienced in complex litigation, data breach cases, and consumer protection class action matters such as this action, and Wooten, Jr. and his counsel intend to vigorously prosecute this action for the Class's benefit and have the resources to do so. Wooten, Jr. and his counsel have no interests adverse to those of the other members of the Class.

62. ***Predominance and Superiority.*** A class action is superior to all other available methods for the fair and efficient adjudication of this controversy because individual litigation of each Class Member's claim is impracticable. The damages, harm, and losses suffered by the individual members of the Class will likely be small relative to the burden and expense of individual prosecution of the complex litigation necessitated by Greylock's wrongful conduct. Even if each Class Member could afford individual litigation, the Court system could not. It would be unduly burdensome if tens of thousands of individual cases or more proceeded. Individual litigation also presents the potential for inconsistent or contradictory judgments, the prospect of a race to the courthouse, and the risk of an inequitable allocation of recovery among those individuals with equally meritorious claims. Individual litigation would increase the expense and delay to all parties and the Courts because it requires individual resolution of common legal and factual questions. By contrast, the class action device presents far fewer management difficulties and provides the benefit of a single adjudication, economies of scale, and comprehensive supervision by a single court.

63. As a result of the foregoing, class treatment under Federal Rule of Civil Procedure 23 is appropriate.

FIRST CLAIM FOR RELIEF
Negligence
(On Behalf of Plaintiff and the Class)

64. Plaintiff incorporates by reference and realleges each of the foregoing paragraphs as if fully set forth herein.

65. In the ordinary course of providing consulting services to its clients and other persons and entities, Defendant solicited, gathered, and stored the PII and PHI of Plaintiff and Class Members. Because Defendant was entrusted with such PII and PHI at all times herein relevant, Greylock owed to Plaintiff and the Class a duty to exercise commercially reasonable methods and care in handling, using, maintaining, storing, and safeguarding the PII and PHI in its care, control, and custody, including by implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that occurred, and to promptly detect and thwart attempts at unauthorized access to its networks and systems. This duty arose independently from any contract.

66. Defendant knew, or should have known, of the risks inherent in collecting and storing massive amounts of PII and PHI, including the importance of adequate data security and the high frequency of ransomware attacks and well-publicized data breaches both generally and the increasing rate of cybercriminals specifically targeting the consulting industry, like Defendant. Greylock owed a duty of care to Plaintiff and Class Members because it was foreseeable that Greylock's failure to adequately safeguard their PII and PHI in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that sensitive information. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and the Class's PII and PHI by failing to limit access to this

information to unauthorized third parties and by not properly supervising both the way the PII and PHI was stored, used, and exchanged, and those in its employ responsible for such tasks.

67. Defendant owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII and PHI. Greylock also owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and circumstances of the Data Breach. This duty is required and necessary for Plaintiff and the Class to take appropriate measures to protect their PII and PHI, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

68. Defendant also had a common law duty to prevent foreseeable harm to others. Defendant had full knowledge of the sensitivity and high value of the PII and PHI that it stored and the types of foreseeable harm and injury-in-fact that Plaintiff and Class Members could and would suffer if that PII and PHI were wrongfully disclosed, leaked, accessed, or exfiltrated. Greylock's conduct created a foreseeable and unreasonable risk of harm to Plaintiff and Class Members, who were the foreseeable victims of Greylock's inadequate data security practices.

69. Defendant violated its duty to implement and maintain reasonable security procedures and practices, including through its failure to adequately restrict access to its file systems and networks that held hundreds of thousands of individuals' PII and PHI or encrypt or anonymize such data. Greylock's duty included, among other things, designing, maintaining, and testing Greylock's information security controls to ensure that PII and PHI in its possession was adequately secured by, for example, encrypting or anonymizing sensitive personal information, installing intrusion detection and deterrent systems and monitoring mechanisms, and using access controls to limit access to sensitive data.

70. Defendant's duty of care also arose by operation of statute, as follows:

a. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard the PII and PHI of Plaintiff and Class Members; and

b. Pursuant to HIPAA, 42 U.S.C. §§ 1320d, *et seq.*, and its implementing regulations, 45 C.F.R. §§ 160, *et seq.*, Defendant had a duty to securely store and maintain the PII and PHI of Plaintiff and Class Members which was collected in conjunction with Defendant's consulting services. Additionally, the HIPAA Breach Notification Rule, 45 C.F.R. § 164.400-414, required Defendant 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."

71. These statutes—the FTC Act and HIPAA—were enacted to protect Plaintiff and the Class Members from the type of wrongful conduct in which Defendant engaged.

72. Defendant breached its duty to exercise reasonable care in protecting Plaintiff's and Class Members' PII and PHI by failing to implement and maintain adequate data security measures to safeguard Plaintiff's and Class Members' sensitive personal information, failing to encrypt or anonymize PII and PHI within its systems and networks, failing to monitor its systems and networks to promptly identify and thwart suspicious activity, failing to delete and purge PII and PHI no longer necessary for its provision of consulting services to its clients and other persons, allowing unmonitored and unrestricted access to unsecured PII and PHI, and allowing (or failing to prevent) unauthorized access to, and copying and exfiltration of, Plaintiff's and Class Members' confidential and private information. Additionally, Defendant breached its duty by utilizing outdated and ineffectual data security measures which deviated from standard industry best practices at the time of the Data Breach. Through these actions, Greylock also violated its duties under the FTC Act and HIPAA.

73. The law imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of PII and PHI to Plaintiff and Class Members so that they can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuses of their private information. Greylock further breached its duties by failing to provide such reasonably timely notice of the Data Breach to Plaintiff and Class Members, including by violating the HIPAA Breach Notification Rule. In so doing, Defendant actually and proximately caused and exacerbated the harm from the Data Breach and the injuries-in-fact of Plaintiff and Class Members. Timely disclosure was necessary so that Plaintiff and Class Members could, among other things: (i) purchase identity theft protection, monitoring, and recovery services; (ii) flag asset, credit, and tax accounts for fraud; (iii) purchase or otherwise obtain credit reports; (iv) place or renew fraud alerts on a quarterly basis; (v) closely monitor loan data and public records; and (vi) take other meaningful steps to protect themselves and attempt to avoid or recover from identity theft and other harms.

74. Public estimates indicate Defendant generates approximately $5 million in annual revenue, and accordingly had the financial and personnel resources necessary to prevent the Data Breach. Greylock nevertheless failed to adopt reasonable data security measures, in breach of the duties it owed to Plaintiff and Class Members.

75. Plaintiff and Class Members had no ability to protect their PII and PHI once it was in Greylock's possession and control. Greylock was in an exclusive position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

76. But for Defendant's breach of its duty to adequately protect Class Members' PII and PHI, Class Members' PII and PHI would not have been stolen. As a result of Greylock's negligence, Plaintiff and Class Members suffered and will continue to suffer the various types of

damages alleged herein. There is a temporal and close causal connection between Greylock's failure to implement adequate data security measures, the Data Breach, and the harms suffered by Plaintiff and Class Members.

77. As a direct and traceable result of Defendant's negligence, Plaintiff and the Class have suffered or will suffer an increased and impending risk of fraud, identity theft, damages, embarrassment, humiliation, frustration, emotional distress, and lost time and out-of-pocket costs to mitigate and remediate the effects of the Data Breach. These harms to Plaintiff and the Class include, without limitation: (i) loss of the opportunity to control how their personal information is used; (ii) diminution in the value and use of their personal information entrusted to Defendant; (iii) the compromise and theft of their personal information; (iv) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and unauthorized use of financial accounts; (v) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including increased costs to use credit, credit scores, credit reports, and assets; (vi) unauthorized use of compromised personal information to open new financial and other accounts; (vii) continued risk to their personal information, at least some of which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the personal information in its possession; and (viii) future costs in the form of time, effort, and money they will expend to prevent, detect, contest, and repair the adverse effects of their personal information being stolen in the Data Breach.

78. Defendant's negligence was gross, willful, wanton, and warrants the imposition of punitive damages given the clear foreseeability of a hacking incident, the extreme sensitivity

of the private information under Defendant's care, and its failure to take adequate remedial steps, including prompt notification of the victims, following the Data Breach.

79. Plaintiff and Class Members are entitled to all forms of monetary compensation set forth herein, including monetary payments to provide adequate long-term identity protection services. Plaintiff and Class Members are also entitled to the injunctive relief sought herein.

SECOND CLAIM FOR RELIEF
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

80. Plaintiff incorporates by reference and realleges each of the foregoing paragraphs as if fully set forth herein.

81. Pursuant to the FTC Act, 15 U.S.C. § 45, Greylock had a duty to maintain fair and adequate computer systems and data security practices to safeguard Plaintiff's and the Class's PII and PHI.

82. 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 Defendant, of failing to use reasonable measures to protect customers' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Greylock's duty to protect Plaintiff's and the Class Members' PII and PHI.

83. Pursuant to HIPAA, 42 U.S.C. §§ 1320d, *et seq.*, Greylock also owed Plaintiff and Class Members a duty to provide adequate data security practices and to safeguard their PII and PHI.

84. Greylock's duty to use reasonable care in protecting confidential and sensitive data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII and PHI.

85. Greylock violated its duties under Section 5 of the FTC Act and HIPAA by failing to use reasonable or adequate data security practices and measures to protect Plaintiff's and the Class's PII and PHI and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII and PHI that Greylock collected and stored and the foreseeable consequences of a cybersecurity data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

86. The harm that has occurred is the type of harm the FTC Act and HIPAA are intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

87. But for Defendant's wrongful and negligent breach of the duties owed to Plaintiff and Class Members, Plaintiff and the Class Members would not have been injured.

88. The injuries and harms suffered by Plaintiff and the Class Members were the reasonably foreseeable result of Defendant's breach of its duties. Greylock knew or should have known that it was failing to meet its duties and that its breach would cause Plaintiff and the Class Members to suffer the foreseeable harms associated with the exposure of their PII and PHI.

89. Defendant's various violations and its failure to comply with the applicable laws and regulations referenced above constitutes negligence *per se*.

90. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII and PHI; harm resulting from damaged credit scores and information; and other

harm resulting from the unauthorized use or threat of unauthorized use of stolen PII and PHI, entitling them to damages in an amount to be proven at trial.

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

THIRD CLAIM FOR RELIEF
Invasion of Privacy
(On Behalf of Plaintiff and the Class)

92. Plaintiff incorporates by reference and realleges each of the foregoing paragraphs as if fully set forth herein.

93. Plaintiff and Class Members have a legally protected privacy interest in their PII and PHI, which is and was collected, stored, and maintained by Greylock, and they are entitled to the reasonable and adequate protection of their PII and PHI against foreseeable unauthorized access, as occurred with the Data Breach.

94. Plaintiff and Class Members reasonably expected that Defendant would protect and secure their PII and PHI from unauthorized parties and that their private information would not be accessed, exfiltrated, and disclosed to any unauthorized parties or for any improper purpose.

95. Greylock unlawfully invaded the privacy rights of Plaintiff and Class Members by engaging in the wrongful conduct described above, including by failing to protect their PII and PHI by permitting unauthorized third parties to access, exfiltrate, copy, and view this private information. Likewise, Greylock further invaded the privacy rights of Plaintiff and Class Members, and permitted cybercriminals to invade the privacy rights of Plaintiff and Class

Members, by unreasonably and intentionally delaying disclosure of the Data Breach, and failing to properly identify what PII and PHI had been accessed, exfiltrated, copied, and viewed by unauthorized third parties.

96. This invasion of privacy resulted from Defendant's failure to properly secure and maintain Plaintiff's and the Class Members' PII and PHI, leading to the foreseeable unauthorized access, exfiltration, and disclosure of this unguarded data.

97. Plaintiff's and the Class Members' PII and PHI is the type of sensitive, personal information that one normally expects will be protected from exposure by the very entity charged with safeguarding it. Further, the public has no legitimate concern regarding Plaintiff's and the Class Members' PII and PHI, and such private information is otherwise protected from exposure to the public by various statutes, regulations, and other laws.

98. The disclosure of Plaintiff's and the Class Members' PII and PHI to unauthorized parties is substantial and unreasonable enough to be legally cognizable and is highly offensive to a reasonable person.

99. Greylock's willful and reckless conduct which permitted unauthorized access, exfiltration and disclosure of Plaintiff's and the Class Members' sensitive, PII and PHI is such that it would cause serious mental injury, shame, embarrassment, or humiliation to people of ordinary sensibilities.

100. The unauthorized access, exfiltration, and disclosure of Plaintiff's and the Class Members' PII and PHI was without their consent, and in violation of various statutes, regulations, and other laws.

101. As a result of the invasion of privacy caused by Defendant, Plaintiff and the Class Members suffered and will continue to suffer damages and injuries as set forth herein.

102. Plaintiff and the Class Members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, restitution, injunctive relief, reasonable attorneys' fees and costs, and any other relief that the Court deems just and proper.

FOURTH CAUSE OF ACTION
Breach of Third-Party Beneficiary Contract
(On Behalf of Plaintiff and the Class)

103. Plaintiff incorporates by reference and realleges each of the foregoing paragraphs as if fully set forth herein.

104. Greylock entered into written contracts with its clients, including with the DOJ, in connection with providing consulting and other professional services. In exchange, Defendant agreed, in part, to implement adequate security measures to safeguard the PII and PHI of Plaintiff and the Class and to timely and adequately notify them of the Data Breach.

105. These contracts were made expressly for the benefit of Plaintiff and the Class, as Plaintiff and Class Members were the intended third-party beneficiaries of the contracts entered into between Greylock and its clients. Defendant knew that, if it were to breach these contracts with its clients, Medicare beneficiaries and other persons, such as Plaintiff and Class Members, would be harmed.

106. Defendant breached the contracts it entered into with its clients by, among other things, failing to: (i) use reasonable data security measures; (ii) implement adequate protocols and employee training sufficient to protect Plaintiff's and the Class's PII and PHI from unauthorized disclosure to third parties; and (iii) promptly and adequately notify Plaintiff and Class Members of the Data Breach.

107. As a direct and proximate result of Greylock's wrongful conduct, Plaintiff and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial, or alternatively, nominal damages. Plaintiff and Class Members are also entitled to

injunctive relief requiring Greylock to strengthen its data security systems, submit to future audits of those systems, and provide adequate long-term credit monitoring and identity theft protection services to all persons affected by the Data Breach.

FIFTH CLAIM FOR RELIEF
Unjust Enrichment / Quasi-Contract
(On Behalf of Plaintiff and the Class)

108. Plaintiff incorporates by reference and realleges each of the foregoing paragraphs as if fully set forth herein.

109. A monetary benefit was directly and indirectly conferred upon Defendant through its receipt of Plaintiff's and Class Members' PII and PHI, which Greylock used to facilitate the provision of consulting services. Greylock appreciated or had knowledge of these benefits conferred upon it by Plaintiff and the Class.

110. Under principles of equity and good conscience, Defendant should not be permitted to retain the full monetary value of the benefits because Greylock failed to adequately protect Plaintiff's and Class Members' PII and PHI.

111. Plaintiff and the Class Members have no adequate remedy at law. Greylock continues to retain some or all of their PII and PHI, exposing this sensitive and private information to a risk of future data breaches while in Defendant's possession. Defendant also continues to derive a financial benefit from using Plaintiff's and Class Members' PII and PHI.

112. As a direct and proximate result of Defendant's wrongful conduct, Plaintiff and the Class Members have suffered various types of damages alleged herein.

113. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds received by it because of its misconduct described herein and the Data Breach.

SIXTH CLAIM FOR RELIEF
Injunctive/Declaratory Relief
(On Behalf of Plaintiff and the Class)

114. Plaintiff incorporates by reference and realleges each of the foregoing paragraphs as if fully set forth herein.

115. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal and state statutes described herein.

116. Defendant owes a duty of care to Plaintiff and Class Members, which required Greylock to adequately monitor and safeguard Plaintiff's and Class Members' PII and PHI.

117. Defendant and its officers, directors, affiliates, legal representatives, employees, co-conspirators, successors, subsidiaries, and assigns still possess some or all of the PII and PHI belonging to Plaintiff and Class Members.

118. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' PII and PHI and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their PII and PHI. Plaintiff alleges that Defendant's data security measures remain inadequate. Furthermore, Plaintiff and the Class continue to suffer injury as a result of the compromise of their PII and PHI and the risk remains that further compromises of their private information will occur in the future.

119. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure the PII and PHI of Plaintiff and the Class within its care, custody, and control under common law, HIPAA, and Section 5 of FTC Act;

b. Defendant breached its duty to Plaintiff and the Class by allowing the Data Breach to occur;

c. Defendant's existing data monitoring measures do not comply with its obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect the PII and PHI of Plaintiff and the Class within Greylock's custody, care, and control; and

d. Defendant's ongoing breaches of said duties continue to cause harm to Plaintiff and the Class.

120. This Court should also issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with legal and industry standards to protect the PII and PHI of Plaintiff and the Class within its custody, care, and control, including the following:

a. Order Defendant to provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

b. Order that, to comply with Defendant's obligations and duties of care, Greylock must implement and maintain reasonable security and monitoring measures, including, but not limited to:

i. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems, networks, and servers on a periodic basis, and ordering

Defendant to promptly correct any problems or issues detected by such third-party security auditors;

ii. Encrypting and anonymizing the existing PII and PHI within its servers, networks, and systems to the extent practicable, and purging all such information which is no longer reasonably necessary for Defendant to provide adequate consulting services to its clients and other persons;

iii. Engaging third-party security auditors and internal personnel to run automated security monitoring;

iv. Auditing, testing, and training its security personnel regarding any new or modified procedures;

v. Segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems, networks, and servers;

vi. Conducting regular database scanning and security checks; and

vii. Routinely and continually conducting internal training and education to inform Defendant's internal security personnel how to identify and contain a data breach when it occurs and what to do in response to a breach.

121. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach or cybersecurity incident. This risk is real, immediate, and substantial. If another Greylock data breach or cybersecurity incident occurs, Plaintiff and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

122. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Plaintiff and the Class will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Defendant's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

123. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent Greylock data breach or cybersecurity incident, thus preventing future injury to Plaintiff and the Class and other persons whose PII and PHI would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class set forth herein, respectfully requests that the Court order the following relief and enter judgment against Greylock as follows:

A. Certifying this action as a class action under Federal Rule of Civil Procedure 23 and appointing Plaintiff and his counsel to represent the Class;

B. Declaring that Greylock engaged in the illegal and wrongful conduct alleged herein;

C. Entering judgment for Plaintiff and the Class;

D. Granting permanent and appropriate injunctive relief to prohibit Defendant from continuing to engage in the unlawful or wrongful acts, omissions, and practices described herein and directing Defendant to adequately safeguard the PII and PHI of Plaintiff and the Class by implementing improved security controls;

E. Awarding compensatory, consequential, and general damages, including nominal damages as appropriate, as allowed by law in an amount to be determined at trial;

F. Awarding statutory or punitive damages and penalties as allowed by law in an amount to be determined at trial;

G. Ordering disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendant as a result of Defendant's unlawful acts and practices;

H. Awarding to Plaintiff and Class Members the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

I. Awarding pre- and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper; and

J. Granting such further and other relief as may be just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury for all claims and issues so triable.

Dated: May 30, 2024

Respectfully submitted,

/s/ Edward F. Haber

Edward F. Haber (BBO# 215620)
Ian J. McLoughlin (BBO# 647203)
Patrick J. Vallely (BBO# 663866)
Shapiro Haber & Urmy LLP
One Boston Place, Suite 2600
Boston, MA 02108
Tel: (617) 439-3939
Fax: (617) 439-0134
ehaber@shulaw.com
imcloughlin@shulaw.com
pvallely@shulaw.com

Amber L. Schubert (*pro hac vice forthcoming)*
Schubert Jonckheer & Kolbe LLP
2001 Union Street, Suite 200
San Francisco, CA 94123
Tel: (415) 788-4220
Fax: (415) 788-0161
aschubert@sjk.law

Counsel for Plaintiff Leland Wooten, Jr. and the Putative Class