IN THE UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF NORTH CAROLINA
DURHAM DIVISION

KIMBERLY FARLEY, CHAD FORRESTER, and KIMBERLY SANDVIG, *on behalf of themselves and all others similarly situated*, Plaintiffs, v. EYE CARE LEADERS HOLDINGS, LLC, Defendant.	Case No. 1:22-CV-00468-UA-JLW **CONSOLIDATED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs, Kimberly Farley, Chad Forrester, and Kimberly Sandvig (collectively, "Plaintiffs") in their individual capacities and on behalf of all others similarly situated, by and through their attorneys, bring this Consolidated Class Action Complaint against Defendant, Eye Care Leaders Holdings, LLC ("ECL" or "Defendant"), and allege, upon personal knowledge as to their own actions, counsels' investigations, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. In 2021, ECL, a record-keeping vendor for top-rated eye care clinics across the country, lost control over millions of patients' highly sensitive personal information for a period of months during a series of ransomware attacks (collectively, the "Data Breach"), then concealed the Data Breach from the public, including its customers and their patients. In fact, ECL itself *never* notified Data Breach victims that cybercriminals had stolen their information. As a result, millions of patients have no idea that cybercriminals gained access to their personally identifiable

information ("PII") and personal health information ("PHI") (collectively, "Private Information" or "PII and PHI"), including their names, birth dates, medical record numbers, health insurance information, Social Security numbers, and medical care information.

2. ECL's customers only just started notifying affected patients about the Data Breach in June 2022, over a year after the Data Breach first occurred. The number of patients known to have been affected by the Data Breach has rapidly swelled to approximately 3 million, putting the Data Breach "on pace to become the largest healthcare data breach in 2022."[1] The number of impacted patients has continued to grow and, consequently, Plaintiffs do not yet know how many were impacted and remain at risk due to the Data Breach.

3. On information and belief, ECL's Data Breach first started in March 2021, when cybercriminals infiltrated ECL's computer systems and crippled a record-keeping system ECL provided to eye care clinics across the country. As a result, ECL lost control over patients' Private Information. ECL obfuscated the nature of the Data Breach to its customers and concealed it from patients, thereby deceiving millions of individuals. On information and belief, ECL at first told its customers that the crippling attack was only a "technical issue," when it knew full well that cybercriminals had successfully attacked its systems.

4. Before ECL could fully restore its systems, on information and belief, cybercriminals breached ECL's systems again just one month later in April 2021. This second incident crippled ECL's electronic medical records systems, interrupting services and exposing even more patient Private Information.

[1] *See* Jessica Davis, *Another 1.3M patients added to data breach tally of ransomware attack on Eye Care Leaders*, SC Media, June 16, 2022, https://www.scmagazine.com/analysis/ransomware/another-1-3m-patients-added-to-data-breach-tally-of-ransomware-attack-on-eye-care-leaders (last visited September 22, 2022).

5. ECL again hid the Data Breach from its customers and patients, depriving patients an opportunity to guard themselves against the Data Breach's devastating impact.

6. On information and belief, in August 2021, four months after the April 2021 hack, ECL's data security measures failed to identify and prevent yet another cybersecurity incident. This time, ECL failed to disable a former employee's company credentials, creating a well-known and significant security vulnerability. Subsequently, the employee, using the valid credentials issued by ECL, accessed ECL's systems and patient's Private Information stored there, allowing the employee to "wreak havoc" using those credentials.[2]

7. Stunningly, ECL's inadequate data security did not stop there. In December 2021, ECL's data security measures failed to identify and prevent a fourth "security incident." ECL reported the breach to eye clinics, including, for example, Texas Tech University Health Sciences Center, EvergreenHealth, Finkelstein Eye Associates, Sylvester Eye Care, Harkins Eye Clinic, Affiliated Eye Surgeons, Chesapeake Eye, Allied Eye Physicians & Surgeons, Inc., and Shoreline Eye Group.[3]

8. ECL's customers have only recently started to notify their patients about the Breach[4] through their own breach notices, disclosing it to millions of patients at a time. Indeed, as of the filing of this Complaint, at least the following ECL customers have disclosed breaches affecting over 2 million patients:

---

[2] *See* Jessica Davis, *Healthcare vendor accused of 'concealed' ransomware, lengthy service outages*, SC Media, April 20, 2022 https://www.scmagazine.com/analysis/incident-response/healthcare-vendor-accused-of-concealed-ransomware-lengthy-service-outages (April 20, 2022).

[3] *See, e.g.*, https://healthitsecurity.com/news/eye-care-leaders-emr-data-breach-tally-surpasses-2-million.

[4] Notifications started in June 2022. After a lull in new reports, Iowa-based Wolfe Clinic, P.C. submitted a breach report on September 9, 2022 to the U.S. Department of Health and Human Services Office for Civil Rights and posted a notice on its website stating that 542,776 individuals were impacted by the Data Breach.

- TTUH Sciences Center (1.29 million patients)
- EvergreenHealth (20,533)
- Allied Eye Physicians & Surgeons (20,651)
- Summit Eye Associates (53,818)
- Affiliated Eye Surgeons (23,400)
- Northern Eye Care Associates (8,000)
- Regional Eye Associates, Inc. & Surgical Eye Center of Morgantown (194,035)
- Frank Eye Center (26,333)
- Ad Astra Eye (3,684)
- Finkelstein Eye Associates (48,587)
- Moyes Eye Center (38,000)[5]
- Sylvester Eye Care (19,377)
- Shoreline Eye Group (57,047)
- AU Health (50,631)
- Associated Ophthalmologists (13,461)
- Kansas City (13,461)
- Fishman Vision (2,646)
- Burman & Zuckerbrod Ophthalmology Associates (1,337)
- McCoy Vision Center (33,930)
- Precision Eye Care (58,462)
- Harkins Eye Clinic (23,993)
- Wolfe Clinic, P.C. (542,776)

9. Thus, the true scope and scale of the Data Breach is still unknown, as is the devastating impact it will have on patients throughout the country.

10. ECL was well-aware of the risks data breaches pose to those who store Private Information, and knew it had a duty to protect that Private Information. By obtaining, collecting, using, and deriving a benefit from the Private Information of Plaintiffs and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

11. The exposed Private Information of Plaintiffs and Class Members can—and likely will—be sold on the dark web. Hackers can offer for sale the unencrypted, unredacted Private Information to criminals. Plaintiffs and Class Members now face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers – the gold standard for identity thieves.

12. This Private Information was compromised due to Defendant's repeated negligence, including its careless acts and omissions, use of foreseeable vulnerable data security measures, and its failure to protect the Private Information of Plaintiffs and Class Members.

[5]*See supra* Fn. 1.

13. ECL's misconduct amounts to negligence and violates state and federal law, having caused injury to patients across the country.

14. Plaintiffs bring this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents.

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

16. Defendant 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 PII and PHI 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 PII and PHI 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 should be entitled to injunctive and other equitable relief.

PARTIES

17. Plaintiff Kimberly Farley is a natural person and citizen of Tennessee, residing in White House, Tennessee, where she intends to remain. Plaintiff Farley is a Data Breach victim and a former patient at Summit Eye Associates ("Summit"), an ECL customer. Plaintiff Farley confirmed she was a Data Breach victim by calling Summit's Data Breach hotline, which confirms whether its patients' information was exposed in ECL's Data Breach.

18. Plaintiff Chad Forrester is a natural person and citizen of Missouri, residing in Park Hills, Missouri, where he intends to remain. Mr. Forrester is a Data Breach victim and a current patient at Precision Eye Care, Ltd, an ECL customer. Mr. Forrester was notified via a Notice of Data Breach Letter, which indicated Defendant maintained Plaintiff Forrester's PII and PHI and failed to protect it in the Data Breach.

19. Plaintiff Kimberly Sandvig is a natural person and citizen of Tennessee, residing in Hermitage, Tennessee, where she intends to remain. Plaintiff Sandvig is a Data Breach victim and a former patient of Summit, an ECL customer. Ms. Sandvig was notified via a Notice of Data Breach Letter, which indicated Defendant maintained Plaintiff Sandvig's PII and PHI and failed to protect it in the Data Breach.

20. Defendant, ECL, is a North Carolina company with its principal place of business at 2222 Sedwick Rd. Durham, North Carolina. ECL's sole "Manager," through whom ECL can be served, is Greg E. Lindberg, at 2222 Sedwick Road, Durham, North Carolina.

JURISDICTION & VENUE

21. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C.§ 1332, at subsection (d), conferring federal jurisdiction over class actions where, as here: (a) there are 100 or more members in the proposed class; (b) at least one member of the class is a citizen of a state different from Defendant; and (c) the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs. *See* 28 U.S.C. § 1332(d)(2) and (6).

22. Upon information and belief, ECL's decisions regarding data security and cybersecurity policies at issue in this matter emanated from this District. Moreover, on information and belief, the server(s) and network(s) at issue were located in this District.

23. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this District.

24. Venue is proper in this District pursuant to 18 U.S.C § 1391(b)(1) because ECL is headquartered and has its principal place of business is in this District, a substantial part of the conduct giving rise to Plaintiffs' claims occurred in this District, and Defendant conducts substantial business in this District.

BACKGROUND FACTS

a. ECL

25. ECL is a practice management and record-keeping service for ophthalmology (eye care) offices throughout the United States.

26. ECL services over 9,000 physicians and provides ophthalmology practice management software and electronic health records system for 40 percent of the eye care market.[6]

27. ECL's website states: "Headquartered in Durham, NC, Eye Care Leaders has brought together leading eye care companies including Integrity, iMedicWare, ManagementPlus, MDOffice, Medflow, My Vision Express, KeyMedical, IO Practiceware, and EyeDoc. We've come together with the common goal of continuing to offer and grow the best eye care solutions available anywhere in the market."[7]

28. ECL advertises that it is a powerful family "of new and existing solutions that can improve, enhance, and coordinate every level of eye care management. The cloud-based suite tightly integrates software that addresses every aspect of the modern eye care practice: revenue cycle, electronic health records, practice management, optical ASC, patient retention, patient reactivation, patient portal, analytics, and more."[8]

29. ECL collects and stores patient PII and PHI on its record-keeping systems from its customers, who collect this information from their patients.

30. More specifically, in the ordinary course of receiving medical records from ECL's customers, ECL was provided with sensitive, personal PII and PHI including names, birth dates, medical record numbers, health insurance information, Social Security numbers, and medical care information.

---

[6] *See HITRUST CSF Certification*, https://eyecareleaders.com/hitrust-csf-certification/ (last accessed: October 20, 2022).
[7] *See* the "About" section on ECL's website, https://eyecareleaders.com/about-eye-care-leaders/ (last accessed Oct. 19, 2022).
[8] *See id*.

31. ECL may also receive PII and PHI from other individuals or organizations that are part of a patient's "circle of care," such as referring physician, patients' other doctors, patient's health plan(s), close friends, or family members.

32. ECL publicly recognizes it has a duty to securely maintain patient Private Information and has published several articles on the critical importance of data security, including "Why You Should Worry About Ransomware," "4 Ways to Protect Your Practice from Ransomware Attacks," and "Six Tips to Improve Patient Data Security for Healthcare Practices."

33. ECL's articles detail why companies that store Private Information have a duty to safeguard such information against theft and explain *how* to safeguard Private Information when they collect it.

34. In fact, in "4 Ways to Protect Your Practice from Ransomware Attacks,"[9] ECL advises readers that as "daunting as these attacks are, knowing what to do and what not to do can make all the difference in whether your practice survives a ransomware attack," listing four security methods:

Get Smart About Ransomware

Education is the most effective defense. A "lack of awareness of healthcare managers regarding the sophistication of hackers" puts many practices at risk, say Campbell and co-presenter Renee Bouvelle, MD. Learn about the latest ways hackers are targeting medical practices, and familiarize your staff with the signs of ransomware:

- inability to open files
- any message about how to pay ransomware
- messages stating 'you have limited time to pay or your files will be deleted'
- a window opening to a suspicious program that you can't close.

[9] *See 4 Ways to Protect Your Practice from Ransomware Attacks*, https://eyecareleaders.com/protect-against-ransomware-attacks/ (last accessed Oct. 19, 2022).

Don't Skimp on Training

Minimize your risk for a ransomware attack by putting in the time and effort to conduct security risk assessments. Hire an outside firm or healthcare security data expert to evaluate the safety of your system each year. "You have to do something else in addition" to endpoint security, says Campbell. "This is not something that your EHR takes care of. This is not a checklist," he warns. Don't skip or shortcut HIPAA/HITECH training, developing and updating HIPAA policies and procedures, or skip developing an "emergency contingency plan." If you haven't paid attention to these things, and a breach does occur, "you can expect a lot more 'help' from the government," Campbell notes.

Keep Your Protection Current

Just like you protect your eyes from the sun with the best UV-blocking sunglasses, you need to protect your IT system with the best anti-virus and anti-malware programs available. It is common to forget or avoid software updates—they can be inconvenient and let's face it, you have more pressing things to do. But by keeping updated and upgrading when necessary, you decrease the risk of a breach that looks for known vulnerabilities in outdated versions of those programs. Your IT professional can guide you to make sure you have the right software for your system.

Build Your Team

As tempting as it may be to watch your bottom line by hiring a general "IT guy" or even a family friend to take charge of your IT department—don't. "Don't hire your cousin's brother-in-law on your mother's side or an IT company that is not trained and skilled in HIPAA, ransomware and digital forensics," warns Campbell. That's like seeing a general surgeon to remove a brain tumor, he says. The right IT professional can even conduct a "penetration test: " They act as a hacker would in order to determine exactly how vulnerable your infrastructure is to a real attack.

35. In another article, "Six Tips to Improve Patient Data Security for Healthcare Practices," ECL lists the six "Tips" as: (i) Perform a security risk assessment; (ii) Train employees on data security protocols; (iii) Establish security guidelines for external devices; (iv) Assign role-based access to data; (v) Encrypt sensitive data; (vi) Build a security first culture.[10]

[10] *See* Six Tips to Improve Patient Data Security for Healthcare Practices, https://eyecareleaders.com/six-tips-to-improve-patient-data-security-for-healthcare-practices/ (last visited Oct. 19, 2022).

36. ECL concludes the article by emphasizing that record keepers must ensure that they safeguard patient data:

> ***Conclusion***
>
> Taking an all-embracing approach to patient data security may seem exhausting, but when sensitive data is at risk, following the above-mentioned best practices can ensure greater protection. For healthcare practices that are planning to take data protection seriously, HIPAA and other regulatory compliance initiatives are a good starting point for building a data security program. However, focus your efforts beyond compliance to ensure that patient data is safe and protected.

37. ECL was aware of its duties to protect the Private Information of Plaintiffs and Class Members and that the failure to do so would create a risk of a data breach. ECL misleads and deceives its customers and their patients through these published articles. Even though ECL claims that it "works in the best interest of eye care practices and ensures operational efficiency, regulatory compliance, and revenue growth," on information and belief, ECL does not follow its own recommended, industry standard practices in securing patient PII and PHI.

b. The Data Breach

38. In March 2021, ECL experienced a ransomware attack that affected its iMedicWare software service, which resulted in an interruption of ECL's services to its customers. On discovering the attack, ECL knew it was a ransomware attack, but did not disclose that fact to its customers or patients. Indeed, ECL at first referred to the attack as a "technical issue."

39. On information and belief, ECL permanently lost control over patient PII and PHI during the ransomware attack.

40. After restoring its systems to some functionality, ECL experienced another attack on April 8, 2021, with cybercriminals once again breaching the iMedicWare software service.

41. On information and belief, the April 2021 attack also exposed patient PII and PHI to cybercriminals. Once again, ECL did not disclose the breach to affected patients, instead choosing to conceal it from them and obfuscate the nature of the breach to its customers.

42. Only four months after the April 2021 hack, in July 2021, ECL experienced yet another data breach. This time, the attack had targeted ECL's myCare Integrity systems. On information and belief, the cybercriminal associated with this attack was a former ECL employee who still maintained ECL login credentials because ECL failed to revoke them. As a result, the former employee had unfettered, illegal access to patient PHI and PII.

43. The security breaches did not stop in July 2021. Despite having experienced at least three breaches during the year, ECL experienced at least one more breach in December 2021 that exposed substantial amounts of patients' Private Information. ECL disclosed this breach to several eye care customers, including, for example, Texas Tech University Health Sciences Center and EvergreenHealth, Finkelstein Eye Associates, Sylvester Eye Care, Harkins Eye Clinic, Affiliated Eye Surgeons, Chesapeake Eye, Allied Eye Physicians & Surgeons, Inc., Shoreline Eye Group, and Wolfe Clinic, P.C.[11]

44. Thus, ECL experienced at least four data breaches in 2021, but disclosed none of the data breaches to the affected patients. Instead, ECL unlawfully punted that responsibility to its customers, who only just began notifying patients about the breach(es) this year.

45. Today, the number of reported ECL Data Breach victims has swelled to approximately 3 million patients.

[11] *See, e.g.,* https://healthitsecurity.com/news/eye-care-leaders-emr-data-breach-tally-surpasses-2-million; https://healthitsecurity.com/news/ia-eye-clinic-adds-543k-to-eye-care-leaders-data-breach-tally#:~:text=September%2021%2C%202022%20%2D%20After%20a,by%20the%20third%2Dparty%20breach.

46. The repeated cybersecurity incidents suggest that ECL *repeatedly* failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over patient PII and PHI. ECL's negligence is evidenced by its failure to prevent at least *four* data breaches in one year, in each case failing to stop cybercriminals from accessing PII and PHI.

47. ECL has refused to disclose the Data Breach to its victims, which is required under both state and federal law.

48. From well-known and highly publicized data breaches on entities similar to ECL, Defendant knew or should have known it would be a target of a data breach. ECL also knew or should have known its security systems were inadequate to prevent a data breach or protect Private Information, and, after its first data breach in 2021, it was on notice that its data security measures were woefully deficient. Yet Defendant failed to take reasonable precautions to safeguard Plaintiffs' and Class Members' PII.

49. Despite the prevalence of public announcements of data breach and data security compromises as well as its own articles on the subject, Defendant failed to take appropriate steps to protect the Private Information of Plaintiffs and Class.

50. To prevent and detect cyber-attacks, Defendant was on notice of, and could have implemented measures recommended by the United States Government, including:

- 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 emails using technologies like Sender Policy Framework

(SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed, and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with the least privilege in mind. If a user only needs to read specific files, the user should not have written 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.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

51. To prevent and detect cyber-attacks, Defendant was on notice of and could have implemented measures recommended by the United States Cybersecurity & Infrastructure Security Agency, including:

- Update and patch your computer. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….
- Use caution with links and when entering website addresses. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net) ….
- Open email attachments with caution. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- Keep your personal information safe. Check a website's security to ensure the information you submit is encrypted before you provide it….
- Verify email senders. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- Inform yourself. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- Use and maintain preventative software programs. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic.

52. To prevent and detect cyber-attacks attacks, Defendant was on notice of and could have implemented measures recommended by the Microsoft Threat Protection Intelligence Team, including:

- Secure internet-facing assets
    - Apply the latest security updates
    - Use threat and vulnerability management
    - Perform regular audit; remove privileged credentials;
- Thoroughly investigate and remediate alerts
    - Prioritize and treat commodity malware infections as a 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 the 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].

53. Given that Defendant was storing the Private Information of millions of patients, Defendant could have and should have implemented all of the above measures to prevent and detect the cybersecurity attacks.

54. Juxtaposed against the basic and inexpensive security measures Defendant was required, but failed, to implement are the immediate, substantial, and long-lasting harms that Plaintiffs and Class Members will suffer due to Defendant's conduct. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cybersecurity attacks, resulting in the Data Breach and the exposure of the Private Information of Plaintiffs and Class Members.

c. Plaintiffs' Experiences

Plaintiff Kimberly Farley

55. Plaintiff Farley is a former patient at an ECL customer, Summit Eye. Summit Eye is a professional Optometrist and Ophthalmologist Corporation in Hermitage, Tennessee. Summit Eye contracted with ECL to provide myCare Integrity, an Electronic Medical Records program.

56. As a condition of receiving Summit's eye care services, Plaintiff Farley was required to disclose her PII and PHI.

57. Plaintiff Farley provided her PII and PHI to Summit Eye and trusted that the information would be safeguarded according to internal policies and state and federal law.

58. In March 2022, ECL informed Summit that the Data Breach affected its patients' files and information, including their names, dates of birth, medical record numbers, health insurance information, Social Security numbers, and information regarding medical care.

59. Plaintiff Farley learned of the Data Breach and confirmed she was a victim by calling a hotline set up by Summit to either confirm or deny whether the Data Breach impacted patients' personal data.

60. Plaintiff Farley is very careful about sharing her sensitive PII and PHI. Plaintiff Farley has never knowingly transmitted unencrypted sensitive PII and PHI over the internet or any other unsecured source.

61. Plaintiff Farley has and will spend considerable time and effort monitoring her accounts to protect herself from identity theft. Plaintiff fears for her personal financial security and uncertainty over what PII and PHI was exposed in the Data Breach. Plaintiff Farley has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data

Breach. This goes far 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.

Plaintiff Chad Forrester

62. Plaintiff Forrester is a current patient at Precision Eye Care Ltd. ("Precision"), an ECL customer. As a condition of receiving Provision's products and services, Plaintiff Forrester disclosed his Private Information.

63. Plaintiff Forrester provided his Private Information to Precision and trusted that the information would be safeguarded according to internal policies and state and federal law.

64. At the time of the Data Breach, ECL retained Plaintiff Forrester's name, address, Social Security number, medical care information, and health insurance information.

65. On June 8, 2022, Precision notified Plaintiff Forrester that ECL's network had been accessed and Plaintiffs' PII and PHI may have been involved in the Data Breach via a Notice of Data Breach letter.

66. Plaintiff Forrester is very careful about sharing his sensitive PII and PHI. Plaintiff Forrester has never knowingly transmitted unencrypted sensitive PII and PHI over the internet or any other unsecured source.

67. Plaintiff Forrester stores any documents containing his sensitive PII and PHI in a safe and secure location or destroys the documents. Moreover, Plaintiff Forrester diligently chooses unique usernames and passwords for his various online accounts.

68. As a result of the Data Breach notice, Plaintiff Forrester spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured. Moreover, this time was spent

at Defendant's direction by way of the Data Breach notice where Defendant advised Plaintiff Forrester to mitigate his damages by, among other things, monitoring his accounts for fraudulent activity.

69. As a result of the Data Breach, Plaintiff Forrester was the victim of a credit card fraud scheme that resulted in an unauthorized and fraudulent charge of $155.30 on his credit card. Specifically, Plaintiff Forrester believes unauthorized third parties used the Private Information disclosed via Defendant's breach to obtain his credit card number and make fraudulent purchases.

70. Plaintiff Forrester suffered actual injury in the form of damages to and diminution in the value of Plaintiff' Private Information—a form of intangible property that Plaintiff Forrester entrusted to Defendant, which was compromised in and as a result of the Data Breach. Plaintiff Forrester suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

71. Plaintiff Forrester has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII and PHI being placed in the hands of unauthorized third parties and possibly criminals.

72. Plaintiff Forrester has a continuing interest in ensuring that Plaintiffs' PII and PHI, which, upon information and belief, remain backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Kimberly Sandvig

73. Plaintiff Sandvig is a former patient of Summit Eye. Summit Eye is a professional Optometrist and Ophthalmologist Corporation in Hermitage, Tennessee. Summit Eye contracted with ECL to provide myCare Integrity, an Electronic Medical Records program.

74. As a condition of receiving eye care services from Summit Eye, Plaintiff Sandvig provided her PII and PHI to Summit Eye, with the expectation that the information would be protected.

75. On or about or about April 27, 2022, Plaintiff Sandvig received a mailed Notice of Data Breach Letter, related to Eye Care Leaders' December 2021 Data Breach.

76. The Notice Letter that Plaintiff Sandvig received listed an extensive amount of her PII and PHI was in files that were "removed" from Eye Care Leaders' network. It stated that her full name was among the files that "may have been accessed or acquired" along with one or more of the following: Social Security number, information regarding care received at Summit Eye, date of birth, medical record number, and/or health insurance information."

77. Plaintiff Sandvig is alarmed by the amount of her Private Information that was stolen or accessed as listed on her letter, and even more by the fact that her Social Security number was identified as among the breached data on Eye Care Leaders' computer system.

78. Since Eye Care Leaders' Data Breach, Plaintiff Sandvig was the victim of identity theft. Specifically, Plaintiff Sandvig's email was hacked. She discovered that someone had accessed her email and changed her email address from "cs.com" to "compuserve.com."

79. After ECL's Data Breach but before she was notified of her PII and PHI being breached, Plaintiff Sandvig noticed that her credit score had plummeted even though she had not changed any of her financial behavior for months. Since learning of the Data Breach, her credit score has gone up some, then back down significantly. She believes the dramatic fluctuations in her credit score are related to ECL's Data Breach.

80. Since the Data Breach, Plaintiff Sandvig has been receiving a significantly higher number of spam emails and texts. She has also received a letter indicating that her PII was recently found on the dark web.

81. Plaintiff Sandvig spends approximately $28 per month on data protection services through her internet service provider and other entities. In addition, she has taken time and changed her passwords on various financial accounts.

82. Since the Data Breach, Plaintiff Sandvig monitors her financial accounts monthly. In particular, Ms. Sandvig goes through her Discover, American Express, Savings, and Checking accounts to ensure she recognizes each charge. She now spends about approximately 15-30 minutes each day inspecting her accounts for unidentified charges, much more than she spent monitoring her accounts in the past. In the months since the Data Breach, she has continuously monitored her accounts to limit her risks.

83. Furthermore, since the Data Breach, Plaintiff Sandvig has been required to take time out of her day to discuss the Data Breach over the phone with Compuserve and McAfee, a virus protection company. Upon information and belief, these discussions each lasted approximately an hour and a half to two hours per call.

84. As a result of the Data Breach, Ms. Sandvig has experienced increased anxiety. Plaintiff Sandvig is aware that cybercriminals often sell Private Information, and that hers could be abused months or even years after a data breach.

85. Had Ms. Sandvig been aware that Eye Care Leaders' computer systems were not secure, she would not have entrusted Eye Care Leaders with her Private Information.

d. Plaintiffs and the Proposed Class Have Suffered Harm Resulting from the Data Breach

86. Plaintiffs and members of the proposed Class have suffered injury from the misuse of their PII and PHI that can be directly traced to Defendant.

87. As a result of ECL's failure to prevent the Data Breach, Plaintiffs and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII and PHI is used;

b. The diminution in value of their PII and PHI;

c. The compromise and continuing publication of their PII and PHI;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended 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 and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII and PHI; and

h. The continued risk to their PII and PHI, which remains in the possession of defendant and is subject to further breaches so long as defendant fails to undertake the appropriate measures to protect the PII and PHI in their possession.

88. Stolen personal information is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

89. The value of Plaintiffs and the proposed Class's personal information on the black market is considerable. Stolen personal information trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

90. It can take victims years to spot identity theft, giving criminals plenty of time to use that information for cash.

91. One such example of criminals using personal information for profit is the development of "Fullz" packages.

92. Cyber-criminals can cross-reference two sources of PII and PHI to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

93. The development of "Fullz" packages means that stolen PII and PHI from the Data Breach can easily be used to link and identify it to Plaintiffs and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII and PHI stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs and other members of the proposed Class's stolen PII and PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

94. The healthcare industry is a prime target for data breaches. Over the past several years, data breaches have become alarmingly commonplace. In 2016, the number of data breaches in the U.S. exceeded 1,000, a 40% increase from 2015.[12] The next year, that number increased by nearly 45%.[13] The following year the healthcare sector was the second easiest "mark" among all major sectors and categorically had the most widespread exposure per data breach. [14]

95. Data breaches within the healthcare industry continued to increase rapidly. According to the 2019 Healthcare Information and Management Systems Society Cybersecurity Survey, 68% of participating vendors reported having a significant security incident within the last 12 months, with a majority of those being caused by "bad actors."[15]

96. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[16] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[17] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30

Gew91[hereinafter "*Data Breaches Increase 40 Percent in 2016*"] (last accessed Sept. 15, 2022).

[12] Elinor Mills, *Study: Medical Identity Theft Is Costly for Victims*, CNET (Mar. 3, 2010), *2018 End-of-Year Data Breach Report*.

[13] *Data Breaches Up Nearly 45 Percent According to Annual Review by Identity Thegt Resource Center® and CyberScout®*, ITRC (Jan. 22, 2018), https://bit.ly/3jdGcYR[hereinafter "*Data Breaches Up Nearly 45 Percent*"] (last accessed Sept. 15, 2022).

[14] *2018 End-of-Year Data Breach Report*, ITRC (Feb. 20, 2019), https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf (last accessed Oct. 19, 2022).

[15] *2019 HIMSS Cybersecurity Survey*, HEALTHCARE INFORMATION AND MANAGEMENT SYSTEMS SOCIETY, INC. (Feb. 8, 2019), https://bit.ly/3LJqUr6 (last accessed Oct. 19, 2022).

[16] *2018 End-of-Year Data Breach Report*.

[17] Elinor Mills, *Study: Medical Identity Theft Is Costly for Victims*, CNET (Mar. 3, 2010), https://cnet.co/33uiV0v (last accessed Oct. 19, 2022).

percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[18]

97. The healthcare industry has "emerged as a primary target because [it sits] on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies to next of kin and credit cards, no other organization, including credit bureaus, ha[s] so much monetizable information stored in their data centers." [19]

98. Charged with handling highly sensitive Private Information including healthcare information, financial information, and insurance information, Defendant knew or should have known the importance of safeguarding the Private Information that was entrusted to it. Defendant also knew or should have known of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Defendant's customers' patients as a result of a breach. Defendant nevertheless failed to take adequate cybersecurity measures to prevent the Data Breach from occurring.

99. As discussed above, Defendant actually counseled others, including its customers, about protecting their data from breaches and ransomware attacks, yet failed to follow its own advice. [20]

100. Defendant now puts the burden squarely on Plaintiffs and Class Members to take steps to protect themselves from the Data Breach. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.5% of U.S.-based workers

[18] *Id.*
[19] Eyal Benishti, *How to Safeguard Hospital Data from Email Spoofing Attacks*, INSIDE DIGITAL HEALTH (Apr. 4, 2019), https://bit.ly/3x6fz08 (last accessed June 10, 2022).
[20] *See supra* Fn. 10.

are compensated on an hourly basis, while the other 44.5% are salaried.[21]

101. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week;[22] leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'"[23] Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

102. Plaintiffs and Class Members are now deprived of the choice as to how to spend their valuable free hours and seek renumeration for the loss of valuable time as another element of damages.

e. Defendant's Actions Violated the Rules and Regulations of HIPAA and HITECH

103. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, et seq. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

---

[21] U.S. BUREAU OF LABOR STATISTICS, Wage Worker Survey, available at https://www.bls.gov/opub/reports/minimum-wage/2020/home.htm#:~:text=In%202020%2C%2073.3%20million%20workers,wage%20of%20%247.25%20per%20hour(last visited Aug. 2, 2022); *see also* U.S. BUREAU OF LABOR STATISTICS, Average Weekly Wage Data, available at https://data.bls.gov/cew/apps/table_maker/v4/table_maker.htm%23type=1&year=2021&qtr=3&own=5&ind=10&supp=0(last visited Aug. 2, 2022) (finding that on average, private-sector workers make $1,253 per 40-hour work week.).

[22] *See* Corey Stieg, *You're Spending Your Free Time Wrong—Here's What t to do be Happier and More Successful*, (Nov. 6, 2019, 1:55 pm) https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html..

[23] *Id.*

104. Defendant is a business associate of a covered entity pursuant to HIPAA. *See* 45 C.F.R. § 160.102. Defendant must therefore comply with the HIPAA Privacy Rule and Security Rule. *See* 45 C.F.R. Part 160 and Part 164, Subparts A through E.

105. Defendant is a business associate of a covered entity pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

106. Plaintiffs' and Class Members' Private Information is "protected health information" as defined by 45 CFR § 160.103.

107. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

108. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

109. Plaintiffs' and Class Members' Private Information is "unsecured protected health information" as defined by 45 CFR § 164.402.

110. Plaintiffs' and Class Members' unsecured protected health information has been acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

111. Plaintiffs' and Class Members' unsecured protected health information acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

112. Plaintiffs' and Class Members' unsecured protected health information that was acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a

result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

113. Plaintiffs' and Class Members' unsecured protected health information was viewed by unauthorized persons in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

114. After receiving notice that they were victims of a data breach that required the filing of a Breach Report in accordance with 45 CFR § 164.408(a), it is reasonable for recipients of that notice, including Plaintiffs and Class Members in this case, to believe that future harm (including identity theft) is real and imminent, and to take steps to mitigate that risk of future harm.

115. The Data Breach could have been prevented if Defendant implemented HIPAA mandated, industry standard policies and procedures for securely disposing of Private Information when it was no longer necessary and/or had honored its obligations to its patients.

116. It can be inferred from Defendant's Data Breach that Defendant either failed to implement, or inadequately implemented, information security policies or procedures in place to protect Plaintiffs' and Class Members' Private Information.

117. Defendant's security failures include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information Defendant creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

d. Failing to implement 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 in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 CFR 164.308(a)(6)(ii);

g. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2);

h. Failing to protect against any reasonably-anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3);

i. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce in violation of 45 CFR 164.306(a)(94);

j. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq*.; and

k. Retaining information past a recognized purpose and not deleting it.

118. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, also required Defendant to provide notice of the breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."

119. Because Defendant has failed to comply with industry standards, while monetary relief may cure some of Plaintiffs and Class Members' injuries, injunctive relief is necessary to ensure Defendant's approach to information security is adequate and appropriate. Defendant still maintains the protected health information and other Private Information of Plaintiffs and Class Members; and without the supervision of the Court via injunctive relief, Plaintiffs' and Class Members' protected health information and other Private Information remains at risk of subsequent Data Breaches.

120. Defendant disclosed the PII and PHI of Plaintiffs and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII and PHI of Plaintiffs and members of the proposed Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII and PHI.

121. Defendant's failure to properly notify Plaintiffs and members of the proposed Class of the Data Breach exacerbated Plaintiffs and members of the proposed Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

CLASS ACTION ALLEGATIONS

122. Pursuant to Federal Rule of Civil Procedure 23(b)(2), 23(b)(3), and 23(c)(4), Plaintiffs bring this action on behalf of themselves and all other persons similarly situated (the "Class"), defined as follows:

> All individuals residing in the United States whose PII and PHI was compromised in the Data Breach affecting ECL, including all persons receiving notice about the Data Breach through ECL's customers.

Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

123. Plaintiffs reserve the right to modify or amend the class definition before the Court determines whether certification is appropriate.

124. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. The Class is so numerous that joinder of all members is impracticable. Upon information and belief, there are millions of individuals whose PII and PHI were improperly accessed in the Data Breach.

b. **Ascertainability**. Class members are readily identifiable from information in Defendant's possession, custody, and control;

c. **Typicality**. Plaintiffs' claims are typical of Class members' claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiffs will fairly and adequately protect the proposed Class's interests. Their interests do not conflict with Class members' interests, and they have retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiffs and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for all Class members. Indeed, it will be necessary to answer the following questions:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiffs and the Class's PII and PHI;

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

iii. Whether Defendant was negligent in maintaining, protecting, and securing PII and PHI;

iv. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

v. Whether the Data Breach caused Plaintiffs and the Class injuries;

vi. What the proper damages measure is; and

vii. Whether Plaintiffs and the Class are entitled to damages, treble damages, or injunctive relief.

125. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible. This action is also appropriate for certification because Defendant has 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. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

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

126. Plaintiffs reallege and incorporate by reference paragraphs 1-125 as if fully set forth below.

127. Defendant owed to Plaintiffs and other members of the Class a duty to exercise reasonable care in handling and using the PII and PHI in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

128. Defendant owed a duty of care to Plaintiffs and members of the Class because it was foreseeable that Defendant'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 PII and PHI —just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and members of the Class's PII and PHI by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

129. Defendant owed to Plaintiffs 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. Defendant also owed a duty to timely and accurately disclose to Plaintiffs and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiffs and members of 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.

130. Defendant owed these duties to Plaintiffs and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiffs and members of the Class's personal information and PII and PHI.

131. The risk that unauthorized persons would attempt to gain access to the PII and PHI and misuse it was foreseeable. Given that Defendant holds vast amounts of PII and PHI, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII and PHI —whether by malware or otherwise.

132. PII and PHI is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII and PHI of Plaintiffs and members of the Class's and the importance of exercising reasonable care in handling it.

133. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII and PHI of Plaintiffs and members of the Class which actually and proximately caused the Data Breach and Plaintiffs and members of the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs and members of the Class's injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and members of the Class

have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

134. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiffs and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII and PHI by criminals, improper disclosure of their PII and PHI, lost benefit of their bargain, lost value of their PII and PHI, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Negligence Per Se
(On Behalf of Plaintiffs and the Class)

135. Plaintiffs reallege and incorporate by reference paragraphs 1-125 as if fully set forth below.

136. 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 Plaintiffs and members of the Class's PII and PHI.

137. 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 or, in this case, patients' PII and PHI. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiffs and the members of the Class's sensitive PII and PHI.

138. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect 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 Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result in the event of a breach, which ultimately came to pass.

139. The harm that has occurred is the type of harm the FTC Act is 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 Plaintiffs and members of the Class.

140. Defendant had a duty to Plaintiffs and the members of the Class to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs and the Class's PII and PHI.

141. Defendant breached its respective duties to Plaintiffs and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs and members of the Class's PII and PHI.

142. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence per se.

143. Defendant's violations of HIPAA and HITECH also independently constitute negligence per se.

144. HIPAA privacy laws were enacted with the objective of protecting the confidentiality of patients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to

healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

145. Plaintiff and Class Members are within the class of persons that HIPAA privacy laws were intended to protect. The harm that occurred as a result of the Data Breach is the type of harm HIPAA privacy laws were intended to guard against.

146. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and members of the Class, Plaintiffs and members of the Class would not have been injured.

147. The injury and harm suffered by Plaintiffs and members of the Class were the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiffs and members of the Class to suffer the foreseeable harms associated with the exposure of their PII and PHI.

148. As a direct and proximate result of Defendant's negligence per se, Plaintiffs and members of 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; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

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

149. Plaintiffs reallege and incorporate by reference paragraphs 1-125 as if fully set forth below.

150. Plaintiffs and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII and PHI and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

151. Defendant owed a duty to its customers and their patients, including Plaintiffs and the Class, to keep this information confidential.

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

153. The intrusion was into a place or thing which was private and entitled to be private. Plaintiffs and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

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

155. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

156. Defendant acted with a knowing state of mind when it failed to notify Plaintiffs and the Class in a timely fashion about the Data Breach, thereby materially impaired their mitigation efforts.

157. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

158. As a proximate result of Defendant's acts and omissions, the private and sensitive PII and PHI of Plaintiffs and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages.

159. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their PII and PHI are still maintained by Defendant with their inadequate cybersecurity system and policies.

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

161. In addition to injunctive relief, Plaintiffs, on behalf of themselves and the other members of the Class, also seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

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

162. Plaintiffs reallege and incorporate by reference paragraphs 1-125 as if fully set forth below.

163. Plaintiffs and members of the Class conferred a monetary benefit upon Defendant in the form of their PII and PHI, as this was used to facilitate payment for Defendant's services.

164. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiffs and members of the Class.

165. As a result of Defendant's conduct, Plaintiffs and members of the Class suffered actual damages in an amount to be determined at trial.

166. Under principals of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and members of the Class because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures for itself that were mandated by federal, state, and local laws and industry standards.

167. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and members of the Class all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT V
Breach of Fiduciary Duty
(On behalf of Plaintiffs and the Class)

168. Plaintiffs reallege and incorporate by reference paragraphs 1-125 as if fully set forth below.

169. In providing their Private Information to Defendant, Plaintiffs and Class Members justifiably placed special confidence in Defendant to act in good faith and with due regard to interests of Plaintiffs and Class Members to safeguard and keep confidential that Private Information.

170. Defendant accepted the special confidence placed in it by Plaintiffs and Class Members. Additionally, although Defendant acknowledges on its website its responsibility to

comply with federal healthcare laws, including the duty to protect Private Information, it failed to do so.

171. There was an understanding between Plaintiffs and the Class Members that Defendant would act for the benefit of Plaintiffs and Class Members in preserving the confidentiality of the Private Information.

172. In light of the special relationship between Defendant and Plaintiffs and Class Members, whereby Defendant became guardian of Plaintiffs' and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its customers' patients, including Plaintiffs and Class Members, for the safeguarding of Plaintiffs and Class Members' Private Information.

173. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its relationships with customers and their patients, in particular, to keep secure Private Information.

174. Defendant breached its fiduciary duties Plaintiffs and Class Members by failing to diligently discovery, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

175. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiffs' and Class Members' Private Information.

176. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

177. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic PHI Defendant created, received, maintained, and transmitted, in violation of 45 C.F.R. § 164.306(a)(1).

178. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1).

179. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1).

180. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents and to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii).

181. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2).

182. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3).

183. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 C.F.R. § 164.306(a)(94).

184. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by impermissibly and improperly using and disclosing PHI that is and remains accessible to unauthorized persons in violation of 45 C.F.R. § 164.502, et seq.

185. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to PHI as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5).

186. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

187. Defendant breached its fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

188. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) 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 and data breach, including but not limited to efforts

spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach and data breach for the remainder of the lives of Plaintiffs and Class Members; and (vii) the diminished value of Defendant's services they received.

189. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and harm, and other economic and non-economic losses.

PRAYER FOR RELIEF

Plaintiffs and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiffs and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII and PHI;

E. Awarding Plaintiffs and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees, costs and expenses, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

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

RESPECTFULLY SUBMITTED AND DATED this 26th day of October, 2022.

/s/ Gary M. Klinger
Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel: 866-252-0878
gklinger@milberg.com

Scott C. Harris
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
900 W Morgan Street
Raleigh, NC 27603
Tel: (919) 600-5003
Fax: (919) 600-5035
sharris@milberg.com

Jean S. Martin
NC 25703
Francesca Kester*
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 559-4908
jeanmartin@ForThePeople.com
fkester@ForThePeople.com

Samuel J. Strauss*
Raina C. Borrelli*
Alex Phillips*
TURKE & STRAUSS LLP
sam@turkestrauss.com
raina@turkestrauss.com
alexp@turkestrauss.com
613 Williamson St., Suite 201
Madison, WI 53703
Telephone (608) 237-1775
Facsimile: (608) 509-4423

Bryan L. Bleichner*
CHESTNUT CAMBRONNE PA
100 Washington Avenue South,
Suite 1700 Minneapolis, MN 55401
Phone: (612) 339-7300
Fax: (612) 336-2940
bbleichner@chestnutcambronne.com
pkrzeski@chestnutcambronne.com

Gary E. Mason
gmason@masonllp.com
Danielle L. Perry*
dperry@masonllp.com
Lisa A. White
lwhite@masonllp.com
MASON LLP
5101 Wisconsin Ave. NW Ste. 305
Washington DC 20016
Phone: 202.640.1160
Fax: 202.429.2294

Ben Barnow*
b.barnow@barnowlaw.com
Anthony L. Parkhill*
aparkhill@barnowlaw.com
Riley W. Prince*
rprince@barnowlaw.com
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
Telephone: (312) 621-2000
Facsimile: (312)641-5504

Joel R. Rhine
NCSB # 16028
Rhine Law Firm, P.C.
1612 Military Cutoff Road
Suite 300
Wilmington, NC 28403
Tel: (910) 772-9960
JRR@rhinelawfirm.com

**pro hac vice applications*

Counsel for Plaintiffs and the Class

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on October 26, 2022 the foregoing document was filed via the Court's ECF system, which will cause a true and correct copy of the same to be served electronically on all ECF-registered counsel of record.

/s/ Gary M. Klinger
Gary M. Klinger

Attorneys for Plaintiffs