THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA
CASE NO: 1:22-CV-00296

ALLIANCE OPHTHALMOLOGY, PLLC; DALLAS RETINA CENTER, PLLC; TEXAS EYE AND CATARACT, PLLC; AND HOFACRE OPTOMETRIC CORPORATION, on behalf of themselves and all others similarly situated, Plaintiffs, v. ECL GROUP, LLC; ECL HOLDINGS, LLC; EYE CARE LEADERS HOLDINGS, LLC; EYE CARE LEADERS PORTFOLIO HOLDINGS, LLC; INTEGRITY EMR, LLC; INTEGRITY EMR HOLDINGS, LLC; ALTA BILLING, LLC; AND ALTA BILLING HOLDINGS, LLC, Defendants.	**SECOND AMENDED CLASS ACTION COMPLAINT**

Plaintiffs, Alliance Ophthalmology, PLLC, Dallas Retina Center, PLLC ("DRC"), Texas Eye and Cataract, PLLC ("TEC"), and Hofacre Optometric Corporation, individually and on behalf a class of those similarly situated, complaining of ECL Group, LLC ("ECL"), ECL Holdings, LLC, Eye Care Leaders Holdings, LLC, and Eye Care Leaders Portfolio Holdings, LLC; DRC, individually and on behalf a class of those similarly situated, complaining against Integrity EMR, LLC and Integrity EMR Holdings, LLC, submit their First Amended Complaint as follows; and TEC and DRC, individually

and on behalf a class of those similarly situated, complaining of Alta Billing, LLC and Alta Billing Holdings, LLC:

INTRODUCTION

It is essential to physicians' practices to know the medical and diagnostic history of every patient the physician treats, not to mention the patient's test results, scans, and other key data critical to the delivery of efficient patient care. However, because physicians are rightly focused on delivering such treatment and care, they often rely on external vendors to provide these record-keeping and related practice management support services.

Here, Plaintiffs, like thousands of other practices, contracted with Defendant ECL, who advertises and offers such services to assist physicians, such as billing, patient record-keeping, and associated practice management support. Plaintiffs relied on ECL to keep their patient records and data and to bill for patient visits, among other administrative tasks. Because these tasks are critical to quality patient care, the parties wrote specific provisions into their contract to control for situations where ECL's systems were out of service.

And that precise scenario came to fruition: ECL suffered an outage as a result of a ransomware attack—a fact it concealed from its clients for weeks. Instead of working diligently to restore service, keeping its clients apprised of such efforts, and mitigating any damages, ECL did the opposite. ECL misrepresented to its clients what truly happened, continually promised service would be restored when it was not (to encourage physicians not to move to new service providers), and invoiced its clients for services that were never provided.

Many of those services remain unavailable months after the outage first occurred. When Plaintiffs expressed to ECL the crippling effect the outage had on their practices and the damages consequently incurred—and that Plaintiffs continue to incur—they were met with silence or misrepresentations. To make matters worse, Plaintiffs continued to endure service outages and were met with further misrepresentations by ECL.

What is more, while by contract the Physicians are entitled to receive their own data for the purpose of transitioning to a new provider, ECL has continually refused to provide such data after repeated demands.

Plaintiffs, on behalf of themselves and other similarly situated practices, thus seek their rightful remedies here and complain of Defendant as follows.

PARTIES

1. Alliance Ophthalmology, PLLC ("Alliance") is a medical provider engaged in the practice of ophthalmology in Fort Worth, Texas.

2. Dallas Retina Center, PLLC is a medical provider engaged in the practice of ophthalmology in Plano, Texas, and Waxahachie, Texas.

3. Texas Eye and Cataract, PLLC is a medical provider engaged in the practice of ophthalmology in Waxahachie, Texas.

4. Hofacre Optometric Corporation ("Hofacre") is a medical provider engaged in the practice of ophthalmology in Chino Hills, California, and San Dimas, California.

5. ECL Group, LLC is a North Carolina limited liability company with its principal place of business in Durham, North Carolina. Greg E. Lindberg is ECL's sole

manager, according to ECL's filings with the North Carolina Secretary of State. Last year, Lindberg was convicted of conspiracy to commit honest services wire fraud and bribery concerning programs receiving federal funds. He was sentenced to 87 months in prison.

6. ECL Holdings, LLC is a North Carolina limited liability company with the same principal place of business and manager as ECL. It is ECL's parent company. (Doc. 10). Upon information and belief, ECL Holdings, LLC is involved in the management of ECL, including with respect to the contracts and fraudulent actions at issue, and holds some of ECL's assets.

7. Eye Care Leaders Holdings, LLC is a North Carolina limited liability company with the same principal place of business and manager as ECL. Upon information and belief, Eye Care Leaders Holdings, LLC is involved in the management of ECL, including with respect to the contracts and fraudulent actions at issue, and holds some of ECL's assets.

8. Eye Care Leaders Portfolio Holdings, LLC is a North Carolina limited liability company with the same principal place of business and manager as ECL. Upon information and belief, Eye Care Leaders Portfolio Holdings, LLC is involved in the management of ECL, including with respect to the contracts and fraudulent actions at issue, and holds some of ECL's assets

9. Integrity EMR, LLC is a North Carolina limited liability company with the same principal place of business as ECL. Upon information and belief, Integrity EMR, LLC licenses or provides to ECL for its use the software that ECL then provided to DRC

and other similarly situated practices as myCare Integrity. Upon information and belief, Integrity EMR, LLC provided all technical services related to myCare Integrity. Upon information and belief, Integrity EMR, LLC, along with ECL, was responsible for maintaining the security of myCare Integrity.

10. Integrity EMR Holdings, LLC is a North Carolina limited liability company with the same principal place of business and manager as ECL. Upon information and belief, Integrity EMR Holdings, LLC is involved in the management of Integrity EMR, LLC, including with respect to its failure to maintain the security of myCare Integrity.

11. Alta Billing, LLC is a North Carolina limited liability company with the same principal place of business as ECL. Its sole member is Greg E. Lindberg. Upon information and belief, Alta Billing, LLC is involved in all revenue cycle management services that ECL provides, along with the development and management of the patient payment portal for practices who have contracted with ECL for revenue cycle management.

12. Alta Billing Holdings, LLC is a North Carolina limited liability company with the same principal place of business and manager as ECL. Upon information and belief, Alta Billing Holdings, LLC is involved in the management of Alta Billing, LLC, including with respect to revenue cycle management services and the failure to maintain security of the patient payment portal for practices who have contracted with ECL for revenue cycle management.

JURISDICTION AND VENUE

13. This Court has personal jurisdiction over Defendants because their principal

place of business is located in this District.

14. This Court has subject matter jurisdiction over this dispute under 28 U.S.C. § 1332 based on complete diversity of the parties and an amount in controversy in excess of $75,000, exclusive of interest and costs.

15. The Court further has jurisdiction over this class action pursuant to 28 U.S.C. § 1332(d) on the grounds that the Class, as defined below, consists of at least 100 plaintiffs, there is diversity of citizenship between the plaintiffs and the defendant, and the aggregate amount in controversy exceeds $5 million.

16. Venue is proper in this Court under 18 U.S.C. § 1391(b)(1) because Defendants' principal place of business is located in this District.

17. In addition, the contracts at issue all specify that any dispute "proceeding under, in connection with, or arising out of" the contracts "shall be instituted only in a court (whether federal or state) located in the State of North Carolina," and thus the Parties agreed and consented to venue and jurisdiction in this District.

GENERAL ALLEGATIONS

18. Plaintiffs entered into contracts with ECL under which ECL agreed to provide two services: (1) revenue cycle management, and (2) maintenance of electronic medical records ("EMR").

19. Through the services it offered, ECL promised to improve the efficiency of Plaintiffs' practices, while helping Plaintiffs improve their collections.

20. In reliance on ECL's representations, Plaintiffs contracted with ECL to

reduce the burden of the billing process, while improving continuity of care through a fluid EMR software system.

I. The EMR Contracts.

21. Alliance, TEC (as the successor in interest to Reagan Eye Center), and other practices entered into substantially similar contracts with ECL under which they purchased licenses to use ECL's iMedicWare EMR software.

22. ECL described its iMedicWare software in its contracts as including, *inter alia*, cloud hosting and backup, an open platform booking sheet manager, adaptive templates, integrated pre-op and post-op patient care, an operative supplies management system, an Aldrete scoring system, real-time audits, patient portal & online scheduling, mobile app access, financial analytic dashboard, optical POS module, inventory & medication management, IRIS Registry Integration, e-prescribing, unlimited real time eligibility checks and direct claim status checks, e-faxing, unlimited equipment integration maintenance, and unlimited non-physician users.

23. Hofacre and other practices entered into contracts with ECL under which they purchased licenses to use ECL's My Vision Express EMR software ("MVE").

24. DRC and other practices similarly entered into contracts with ECL under which they purchased licenses to use ECL's myCare Integrity EMR software (myCare Integrity, iMedicWare, and MVE, collectively, "EMR software"). ECL described myCare Integrity in its contracts as providing practice analytics, eRx, basic myCare patient portal, ICD10 data dictionary, and direct messaging. Integrity EMR, LLC provided ECL with all

technical support services related to myCare Integrity.

25. Upon information and belief, ECL used substantially the same contracts with all practices that purchased licenses to use ECL's EMR software.

26. Pursuant to those contracts, Plaintiffs and other practices paid ECL both a one-time fee and monthly fee for their EMR software license.

27. ECL agreed to provide its EMR software "in accordance with the Service Level Addendum" ("SLA"). Under the SLAs, ECL agreed to "use commercially reasonable efforts to make the [EMR] Software available 99% of the time," as measured on a monthly basis. However, no downtime due to *scheduled* maintenance or a force majeure event counted against the 99% threshold.

28. In the event of an issue impacting "performance, utility, or functionality" of the EMR software, ECL agreed to fix the issue within:

- 1 hour if the issue was "loss or interruption of accessibility of the Software" due to ECL's failures;
- 12 hours if the issue was a defect that did not cause losses or interruptions of accessibility of the Software, but that could cause such issues if not corrected, such as one or more systems being down; and
- 72 hours if the issue was a defect that did not cause loss or interruption of accessibility of the Software, but involved failure of a device or subsystem that had minor impact on site functionality and had not resulted in any performance degradation.

29. In recognition of the importance of ensuring the accessibility and functionality of the EMR software, ECL agreed in its contracts for EMR software to reduce monthly subscription fees by 10 - 50% in the event that the EMR software was available less than 95% of the time measured over a calendar month.

30. ECL also agreed to perform its duties in compliance with applicable federal, state and local laws, rules, and regulations.

31. Indeed, maintaining the security of confidential, personally identifiable, and protected health information is a critical issue in the health care industry, especially due to the myriad of regulations governing same, including the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). This is also a significant reason why many health care providers, such as Plaintiffs, contract with third-party EMR vendors to ensure the security of their patient data.[1]

32. ECL therefore agreed to "maintain the security of [patient] data using industry-standard data security protocols, and other methods reasonably deemed to be adequate for secure business data." Importantly, ECL also agreed to notify [licensees] in the event of a breach of security involving [patient] data." With respect to myCare Integrity, Integrity EMR, LLC was responsible for maintaining the security of the software.

33. ECL further agreed to "retain [patient] data on a secure server and to maintain data recovery and data backup facilities in accordance with accepted industry practices."

[1] Indeed, HIPAA directly applies to business associates such as ECL explicitly because so many physicians rely on such vendors. 45 C.F.R. § 164.104(b).

34. Moreover, ECL agreed "not to reveal or disclose any Confidential Information of licensees for any purpose," except as otherwise permitted. None of the contractual exceptions apply here.

35. In connection with its EMR contracts, ECL entered into HIPAA Business Associate Agreements ("BAAs") with its licensees, such as Plaintiffs. Under the BAAs, ECL agreed to not use or disclose protected health information except for limited purposes.

36. Under the BAAs, ECL agreed "to use appropriate safeguards, and comply with Subpart C of 45 C.F.R. Part 164 with respect to electronic [protected health information], to prevent use or disclosure of [protected health information] other than as provided for by the BAA." Specifically, ECL agreed to "use appropriate administrative, physical, and technical safeguards to (a) maintain the security of the [protected health information] and (b) prevent the use and disclosure of [protected health information]." With respect to myCare Integrity, Integrity EMR, LLC was responsible for maintaining the security of the software through the above actions.

37. Under the BAAs, ECL agreed to "report promptly" to licensees "any use or disclosure of the [protected health information] not provided for by this BAA of which it becomes aware, including breaches of unsecured [protected health information], and any security incident of which it becomes aware." ECL agreed that its report "shall include" a "brief description of what happened" and a "description of the types of [protected health information] that were involved." ECL also agreed to provide "any additional information reasonably requested by [licensees] for purposes of investigating the breach."

38. Under the BAAs, ECL agreed to indemnify, defend, and hold licensees harmless for "any loss, claim, damage, or liability" proximately caused by ECL's (1) violation of a material term of the BAA, (2) violation of HIPAA, or (3) gross negligence or willful misconduct.

39. Upon information and belief, other than varying levels of software services and compensation terms, each of ECL's EMR contracts with physician practices contain the same material terms.

II. The Revenue Cycle Management Contracts.

40. ECL also agreed under its EMR contracts to provide revenue cycle services to licensees related to billing for, *inter alia*, ambulatory surgery centers, injectable drugs, and non-insurance procedures, services, or products paid for by the patient, along with claim submission and patient billing and statements, reports, and account management services.

41. As compensation for ECL's revenue cycle services, licensees agreed to pay ECL a percentage of net collections for the billings ECL managed.

42. Alta Billing, LLC and Alta Billing Holdings, LLC actually provided the revenue cycle services on behalf of ECL.

III. ECL's iMedicWare Breach and Mismanagement.

43. In or about March 2021, ECL experienced a ransomware attack that impacted iMedicWare.

44. TEC notified ECL that it was unable to bill for testing due to recent

iMedicWare failures after an update, which caused complete disorganization of TEC's with patient files and medical records.

45. iMedicWare was inaccessible to licensees for between four (4) and seven (7) days. This outage caused severe disruption to licensees' practices because they could not access patient data during this period.

46. Rather than be transparent about experiencing a ransomware attack, ECL initially tried to hide what happened from its clients in order to keep them from exercising their remedies under the EMR contracts and to avoid having to make the fee concessions required under those contracts.

47. After Alliance notified ECL of the outage it was experiencing at 5:30 a.m. on March 22, 2021, ECL acknowledged the outage and claimed the system would be restored that day. But access was not restored that day.

48. Nor was access restored the next day, when ECL again acknowledged an issue with iMedicWare, but did not disclose the ransomware attack.

49. Indeed, ECL continued to falsely claim via mass emails to licensees the outage was a "technical issue," when in reality ECL knew it was the result of a ransomware attack.

50. ECL also continued to claim via mass email to licensees that access and functionality would be restored soon thereafter. And after each promised restoration date passed, ECL moved the goalposts.

51. This left licensees' practices in a state of flux and hostage to ECL's limited

communications and misrepresentations when it did communicate. Licensees could do nothing other than rely on ECL to plan and schedule for their practices during this period. They made plans based on ECL's representations about when iMedicWare would be restored, and then had to change their plans to match ECL's shifting representations.

52. For example, ECL sent the following mass emails to licensees from its imwsupport@eyecareleaders.com that contained intentional omissions and material misrepresentations:

- March 22, 2021 at 8:04 AM: "myCareiMedicWare is aware of the technical issues that your practice is experiencing currently. This issue is diligently being worked on by our hosting team. We apologize for the inconvenience to your practice."

- March 22, 2021 at 12:38 PM: "We are continuing to work on resolving the outage you are experiencing. We anticipate having full service restored **prior to the start of business, Tuesday, March 23rd**. If there are any changes to this timeline, we will notify you promptly." (emphasis in original).

- March 23, 2021 at 5:32 AM: "The technical team's is actively working on resolving the outage/performance issues you are currently experiencing. We apologize for the delay in resolution and will continue to provide updates as soon as possible."

- March 23, 2021 at 10:24 AM: "Monday morning we experienced a significant issue in the data center that hosts your instance of myCare iMedicWare. . . . To set expectations properly, we do anticipate downtime and performance lags to continue through the day today **but expect to have everything resolved overnight tonight. In anticipation of the question, please rest assured that no data has been lost or compromised**. . . . We are doing everything we can to restore full service to your practice as quickly as humanly possible." (emphasis added).

- March 23, 2021 at 3:51 PM: "**All users should be up and running no later than mid-day Thursday**. . . . Please know we are and will be doing everything we can to beat that timeline."

- March 24, 2021 at 6:30 AM: "**All users should be up and running no later than mid-day Thursday.** . . . Please know we are and will be doing everything we can to beat that timeline."

- March 25, 2021 at 4:52 PM: "myCare iMedicWare is aware of the technical issues that your practice may be experiencing currently. The issue is diligently being worked on by our hosting team."

- March 26, 2021 a 11:49 AM: "Our hosting team continues to work on resolving the technical issues that your practice may be experiencing currently."

53. Finally, nearly a week after the ransomware attack, ECL finally informed its licensees via mass email on March 26 that iMedicWare had suffered a ransomware attack. ECL also admitted that some of its databases were corrupted or encrypted by the ransomware.

54. Even after the initial outages, it took more than 30 days for ECL to restore some of the functionality and services of iMedicWare that ECL agreed to provide under the contracts.

55. As an example, the skeleton version of iMedicWare restored after the ransomware attack prevented licensees from updating patient files and medical records through the software, billing for services through the software, scheduling surgeries through the software, and communicating with patients through the software.

56. There were also numerous shorter outages throughout April. On April 8, 2021, ECL experienced another ransomware attack that impacted iMedicWare. There were subsequent outages on April 13, 16, 20, 26, and 27. Each outage impacted licensees'

practices. As an example, TEC had to stop a scheduled surgery the morning of April 27, 2021, due to the outage.

57. A few months later, on June 7, 2021, iMedicWare suffered another significant outage for three days.

58. Despite ECL's obligation to maintain cloud hosting and backup, retain patient data on a secure server, and maintain data recovery and data backup facilities, ECL *never* recovered patient data from March 15, 2021 to March 19, 2021. Thus, licensees' patient data for that week is permanently lost. And without patient records, some licensees could not bill for services they provided that week.

59. ECL's iMedicWare failures breached its obligations under the contracts related to security of information, software availability, software functionality, and defect resolution periods.

60. And despite knowing that it had experienced an attack, ECL intentionally omitted this fact in its communication with its clients and misrepresented the attack as a mundane "technical issue." ECL further misrepresented that "no data has been lost or compromised" when, in reality, ECL had lost and never recovered patient data from March 15-19, 2021. ECL also misrepresented how long it would take to restore functionality and did not satisfy any of its timeframes. At all times, ECL had a duty to disclose to licensees that it had experienced an attack and that data may be compromised or lost.

61. ECL's material omissions and misrepresentations were intentional and made in an attempt to retain the licensees and to induce them to continue their contractual

relationship with ECL. Licensees relied on the intentional omission and misrepresentations by ECL to believe that no attack had occurred, that functionality would be restored as promised, and that they should continue their contractual relationship with ECL. As a result of ECL's fraudulent omissions and representations and licensees reasonable reliance on same, licensees suffered damages.

62. Despite all of these failures and the failure to provide functioning and accessible iMedicWare service for at least 95% of the month, as specified in the contracts, ECL continued to invoice licensees for the full monthly service fee as if nothing had happened.

63. Patients lost confidence in licensees' practices due to these outages and lack of functionality, which deprived licensees of the ability to schedule with certainty, review preexisting appointments and prepare for same, review patient information, and input data into the software.

64. Ultimately, patients left licensees' practices due to the continued negative impact of ECL's failures. ECL's failures also harmed licensees' reputations and abilities to attract new patients.

65. In addition, despite being obliged to reduce or forgive licensing fees for its software to reflect the outages, ECL falsely reported to collections agencies, credit agencies, and others, that Plaintiffs had failed to pay their bills, and referred their accounts to collections agents. Plaintiffs were damaged by these false statements, were forced to incur expenses responding to ECL's false claims, and their credit scores were impacted,

increasing the costs of credit.

66. ECL's failure to restore full functionality has also caused licensees other and additional damages. Among other things, ECL's failures have denied licensees access to data necessary to submit required reports to The Centers for Medicare & Medicaid Services ("CMS"), resulting in the loss of incentive payments under the Medicare Merit-Based Incentive Payment System, and requiring licensees to incur expenses necessary to obtain hardship exceptions to the CMS reporting requirements.

67. To address the outages and lack of functionality, licensees also had to either hire new staff or pay overtime for existing employees to manually enter data and manually manage payments and scheduling, including the use of paper records.

68. ECL's repeated failures eventually forced some licensees to transition to a new EMR software provider, which led to those licensees incurring significant transition costs.

69. Upon information and belief, ECL Holdings, LLC, Eye Care Leaders Holdings, LLC, and Eye Care Leaders Portfolio Holdings, LLC participated in and orchestrated the aforementioned fraudulent conduct in concert with ECL.

IV. ECL's myCare Integrity Breaches and Mismanagement.

70. Integrity EMR, LLC, along with ECL, were responsible for maintaining the security of sensitive data of practices' patients, including protecting myCare Integrity from ransomware attacks. They failed to do so.

71. On August 17, 2021, ECL experienced an attack that impacted myCare

Integrity.

72. According to an email ECL sent to licensees on August 28, 2021 at 2:07 PM, ECL "*immediately* identified and stopped the source of the attack." (emphasis added). Despite knowing about the attack "immediately," ECL did not immediately disclose that it had been subject to an attack, instead intentionally omitting this information and misrepresenting the nature of the myCare Integrity system issues in mass emails to licensees.

73. Indeed, from August 20, 2021 to August 27, 2021, ECL sent numerous mass emails to licensees about the issues myCare Integrity was experiencing. These communications falsely characterized the issue as a "performance" or "system" issue when ECL knew it was actually caused by a ransomware attack. None of these communications notified licensees that ECL had been the subject of an attack. For example, ECL sent the following emails containing material omissions and misrepresentations to its licensees from its mycareintegritysupport@eyecareleaders.com address:

- August 20, 2021 at 8:22 AM: "Some of our customers may be currently experiencing performance issues within the Integrity HER and possible connection loss with the Integrilink device. We apologize for any system issues that you may be currently experiencing as we work to resolve these issues. In an effort to provide open communication, we want to inform you that we are working with our development team and third-party resources to ensure you are able to provide the best care for your patients. We will continue to provide updates as they are available."

- August 26, 2021 at 7:02 AM: "Some of our users may be experiencing intermittent system issues. Our development team is working diligently to resolve the issue. We appreciate your patience as we work to resolve the issue."

- August 26, 2021 at 9:22 AM: "Some of our users may be experiencing intermittent system issues. Our development team is working diligently to resolve the issue. We appreciate your patience as we work to resolve the issue."

- August 26, 2021 at 3:10 PM: "Our development team is diligently working to resolve the issues that some users may be experiencing. We apologize for the inconvenience and thank you for your patience. We will continue to share updates as soon as they are available."

- August 27, 2021 at 7:07 AM: "Our development team continues to work diligently work to resolve the issues that some users may be experiencing. We apologize for the inconvenience and thank you for your patience. We will continue to share updates as soon as they are available."

- August 27, 2021 at 4:42 PM: "Our development team continues to work diligently work to resolve the issues that some users may be experiencing. We apologize for the inconvenience, and thank you for your patience. We will continue to share updates as soon as they are available."

- August 28, 2021 at 12:06 PM: "Our development teams continue to work to resolve the issues that some users may be experiencing. We apologize for the inconvenience and will continue to share updates as soon as they are available."

74. Finally, on August 28, 2021 at 2:07 PM, ECL informed licensees via a mass email that it had experienced an attack.

75. Again, by ECL's own words, it knew about the attack immediately. ECL, however, intentionally omitted this fact in its communication with its clients and misrepresented the attack as a routine "performance issue." ECL further misrepresented that it would "share updates as soon as they are available" when, at the time of this statement, ECL knew that it had experienced an attack and yet did not disclose that update until 11 days after it learned of the attack.

76. ECL intentionally omitted information about the attack despite a duty to inform the licensees of same. ECL also intentionally omitted information and misrepresented the nature of the attack in an attempt to retain the licensees and to induce them to continue their contractual relationship with ECL. Licensees relied on the intentional omission and misrepresentations by ECL to believe that no attack had occurred, that functionality would be restored, and that they should continue their contractual relationship with ECL. As a result of ECL's fraudulent omissions and representations and licensees reasonable reliance on same, licensees suffered damages.

77. Upon information and belief, the attack was by a former ECL employee. After this employee stopped working for ECL, ECL negligently failed to revoke the employee's credentials and prohibit the employee from accessing ECL's systems. The former employee then exploited the unrevoked access to create a backdoor to access practices' and patients' EMR data. This vulnerability exposed, and therefore constitutes the written publication of, data in violation of the practices' and patients' right of privacy. Competitors could have accessed this data to identify the practices' lists of patients. Other bad actors could have accessed the data to commit identity theft. Thus, ECL's own former employee accessed its systems and wreaked havoc using the employee's prior credentials. ECL could have prevented this by simply revoking the employee's credentials at the time of separation, like every well-run company. But it failed to do so, resulting in systemwide outages for more than a month. This was not a sophisticated cyberattack; it was negligent supervision. ECL's, Integrity EMR, LLC's, and Integrity EMR Holdings, LLC's

negligence violated the myCare Integrity licensees' right of privacy and caused them damages in the form of (a) having to engage privacy professionals to ensure compliance with applicable laws, (b) having to research and determine whether their data had been compromised by exploitation of the vulnerability and written publication, (c) having to incur additional fees to transfer to a more reliable EMR vendor, (d) having to engage in additional security measures to protect their data; (e) having to spend additional resources to collect and manage EMR records outside of myCare Integrity while the software was not functional.

78. Even after ECL finally disclosed the attack, it continued to misrepresent the extent of the attack and how long it could take to restore access to and the functionality of myCare Integrity, noting only via mass email that it was "diligently working to resolve the issue." ECL knew that access and functionality would not be restored within a matter of days, yet it did not immediately disclose this to clients. ECL effectively hid from licensees that the widespread outages it was experiencing would last for weeks on end. For example, ECL sent the following emails containing material omissions and misrepresentations to its licensees from its mycareintegritysupport@eyecareleaders.com address:

- August 28, 2021 at 2:07 PM: "The exact timeframe for the Integrity restoration remains pending. Our development, operations, and security teams are working diligently to restore the system quickly and safely."

- August 30, 2021 at 2:23 PM: "The exact timeframe for the Integrity restoration remains pending. Our development, operations, and security teams are working diligently to restore the system quickly and safely."

- August 31, 2021 at 4:26 PM: "The exact timeframe for the Integrity restoration remains pending. Our development, operations, and security teams are working diligently to restore the system quickly and safely."

- September 3, 2021 at 8:42 AM: "Our development, operations, and security teams continue to work diligently to fix the coding issues and bring Integrity back online safely. The timeframe for restoration remains pending, and we will update you when we are able to provide a more definitive ETA."

- September 3, 2021 at 4:43 PM: "Our development, operations, and security teams continue to work diligently to fix the coding issues and bring Integrity back online safely. The timeframe for restoration remains pending, and we will update you when we are able to provide a more definitive ETA."

79. On September 8, 2021 at 8:41 PM, ECL finally disclosed in a mass email to clients that it "expect[ed] full access restoration to take time on the order of weeks rather than days."

80. Upon information and belief, ECL knew this at the time of its above emails and intentionally omitted and misrepresented the amount of time to restore access in an attempt to retain the licensees and to induce them to continue their contractual relationship with ECL. Licensees relied on the intentional omission and misrepresentations by ECL to believe functionality would be restored "quickly," and that they should continue their contractual relationship with ECL. As a result of ECL's fraudulent omissions and representations and licensees reasonable reliance on same, licensees suffered damages.

81. Because the practices had little details about the ransomware attack, despite representations from ECL that no patient data had been compromised, each practice had to

expend significant time and resources ensuring they complied with their HIPAA obligations and state law disclosure obligations.

82. Moreover, the practices had a duty to ensure there was no risk to patient safety or continuity of care, and thus had to spend significant sums ensuring they complied with that duty.

83. In late September, more than a month after the initial attack, ECL finally rolled out a "viewer" that would at least allow licensees to view limited patient information. The viewer, however, had no other functionality. Indeed, licensees still could not view scans and other important images.

84. In short, for months on end, licensees' practices were crippled due to ECL's and Integrity EMR, LLC's failures to maintain security of their patient information and access and functionality of myCare Integrity.

85. Licensees could not access any patient information for more than a month; they had to convert to a paper and manual entry system for ongoing visits, and they could no longer send correspondence electronically through the software.

86. Ultimately, patients left some licensees' practices because of ECL's continued failures, which dramatically undermined licensees' physician-patient relationships and care.

87. To date, full functionality of myCare Integrity has not been restored.

88. Moreover, when DRC attempted to transition to a new EMR software provider due to ECL's failures, ECL could not export DRC's patient data.

89. Then, in April 2022, ECL sent myCareIntegrity clients by certified mail an undated and unsigned letter with no header or footer providing any contact information. The subject of the letter was "Re: Supplemental IT Incident Information." The problem is that this was not, in fact, "Supplemental" information and was, instead, the *first* notification.

90. The letter revealed that, on December 4, 2021, myCareIntegrity's "electronic health record application was the subject of a security incident where an unknown attacker accessed the Integrity back-end and deleted databases and system configuration files." The letter acknowledged that this caused "interruption to" licensees "clinical practice."

91. Despite ECL's obligation to maintain cloud hosting and backup, retain patient data on a secure server, and maintain data recovery and data backup facilities, the letter admitted that ECL did not yet know whether it would be able to restore all databases. Integrity EMR, LLC's negligence contributed to this issue.

92. To make matters worse, ECL lied about the breach and failed to disclose the nature of the December event until months later.

93. Specifically, ECL's April letter stated that, "upon detecting the attack, ECL's response team disabled the attacked instance, revoked access to it, and forced password changes." The letter also states that the attack "was detected in less than twenty-four (24) hours." Yet despite knowing in less than 24 hours that an attack had occurred on December 4, ECL lied to licensees, telling them that it was just "experiencing intermittent system issues." For example, ECL sent the following emails containing material omissions and

misrepresentations to licensees from its mycareintegritysupport@eyecareleaders.com address:

- December 5, 2021 at 9:59 AM: "Some of our users may be experiencing intermittent system issues. Our development team is working diligently to resolve the issue. We will continue to share updates as soon as they are available. We apologize for the inconvenience and thank you for your patience as we work to resolve the issue."

- December 6, 2021 at 8:51 AM: "Our development team is diligently working to resolve the issues that some users may still be experiencing with opening PDF documents, and opening prior encounters. We apologize for the inconvenience and thank you for your patience. We will continue to share updates as soon as they are available."

- December 7, 2021 at 6:57 PM: "We are writing to provide a short update on the recent disruption to the myCare Integrity platform. We understand that your system is still experiencing issues and we want to assure you that we are working to resolve this as soon as possible. We have re-engaged our third-party technical experts to investigate the issue and restore your service and backups as quickly and safely as we can. *We are sure that you have questions about the technical details, the exact cause of this new issue, and the impact to your systems and data. In our communications, we strive to present only verifiable facts and to avoid speculation because you deserve an accurate picture of the situation. As our expert response team discovers and confirms information about the cause, impact, and restoration, we will provide you with details as we are able.* Below is the list of known issues as of today: General issue with red-bar errors occurring while navigating through the site; Issues opening prior encounters, generating PDFs, and closing encounters ; ICD-10 error messages within encounters; Issues opening correspondence from Patient Dashboard on prior encounters; Issues with uploading and viewing images and documents in Document Center and IntegriView; Practice Management integration issues, including issues with updating Patient Demographics and Scheduling within Integrity; Issues populating data in Integrity's Coding Integration Report; Issues with some fields within prescription ordering screens. *We will continue to communicate with you regularly and to provide substantive updates on the situation as soon and often as we can.* We are committed to continuing to provide service and support to your practice and the myCare Integrity staff remains available to assist you however we can." (emphasis added)

- December 8, 2021 at 8:30 AM: "Our development team is diligently working with AWS to resolve the issues that our users are currently experiencing. Again, we apologize for the inconvenience and thank you for your patience as we work to resolve this in a timely manner. We will continue to share updates as soon as they are available."

94. Again, by ECL's own words, it detected and knew about the attack on December 4, 2021, in less than 24 hours. ECL, however, intentionally omitted this fact in its communication with its clients and misrepresented the attack as a run-of-the-mill system interruption. ECL intentionally omitted information about the attack despite a duty to inform the licensees of same. ECL also intentionally omitted information and misrepresented the nature of the attack in an attempt to retain the licensees and to induce them to continue their contractual relationship with ECL. Licensees relied on the intentional omission and misrepresentations by ECL to believe that no attack had occurred, that their patients' data had not been compromised, that databases would be restored, and that they should continue their contractual relationship with ECL. As a result of ECL's fraudulent omissions and representations and licensees reasonable reliance on same, licensees suffered damages.

95. This breached ECL's obligations under the EMR contracts, under which ECL agreed to provide an export of patient data at no expense. Upon information and belief, Integrity EMR, LLC, Integrity EMR Holdings, LLC, ECL Holdings, LLC, Eye Care Leaders Holdings, LLC, and Eye Care Leaders Portfolio Holdings, LLC participated in and orchestrated the aforementioned fraudulent conduct in concert with ECL.

V. ECL's MVE Breaches and Mismanagement.

96. As with iMedicWare and myCare Integrity, MVE experienced multiple ransomware attacks that ECL initially disguised as rudimentary functionality issues.

97. The first was in late 2019.

98. On November 28, 2019, ECL sent a mass email to MVE users informing them that "[s]ome of our cloud users may be experiencing issues accessing My Vision Express. We are working diligently to resolve the issue. We will notify you as soon as the functionality is fully restored."

99. The next day, ECL identified that it had experienced a ransomware attack, but stated that "[c]lient and patient data have not been compromised." Though no patient data was impacted or compromised, full functionality was not restored until December 12.

100. The end of a year is a busy and critical period for practices, as patients have often used their insurance deductible and therefore schedule visits before their deductible resets. Thus, this two-week outage in late 2019 caused substantial damages to the MVE users, especially given that ECL initially claimed via mass email that functionality would be restored in 24 hours. Yet ECL failed to reduce the monthly service fee for this outage as required under its MVE contracts.

101. In October and November 2020, MVE experienced additional outages. And ECL again failed to reduce the monthly service fee for the outages as required under its MVE contracts.

102. In March and April 2021, MVE experienced successful ransomware attacks

that ECL failed to disclose until more than two months later.

103. Knowing that it had experienced successful ransomware attacks, ECL sent a mass email on May 21, 2021 that MVE "servers have been taken down for unplanned but necessary maintenance." This was, in actuality, due to the prior ransomware attacks—not routine maintenance.

104. The next three days, ECL sent mass emails that: "Our team continues to conduct maintenance on our MVE servers"; "Our team continues to conduct maintenance on our MVE servers"; and "Our team has completed the maintenance on the servers." Again, this was due to ransomware attacks—not routine maintenance.

105. On June 3, 7, and 8, ECL sent mass emails with more of the same: "On Saturday, June 5th, our Data Center and Network team will be conducting some scheduled maintenance"; "Our team is conducting maintenance on our MVE servers. Your system will be temporarily unavailable. We will share a firm time frame as to when the functionality will be restored as soon as it is available."; and "The My Vision Express team will be conducting system maintenance over the next few weeks. This maintenance will include security updates that will help to reinforce our firewalls. Your system will intermittently be unavailable at times."

106. Finally, on June 9, ECL informed MVE users that it had experienced recent "***attempted*** attacks on our systems" and that it "took MVE offline to take preventative security measures to protect your patients' health information. This was a proactive measure intended to protect you, your practice, and your patients." (emphasis added). ECL,

however, failed to disclose that the "attempted" attacks were, in fact, successful ransomware attacks.

107. Two weeks later, on June 24, ECL finally came clean. It informed ECL users by mass email that some ECL "servers were encrypted by malicious ransomware attacks on March 21 and April 8, 2021." To address the attacks, ECL stated that it would "invest in, upgrading our cyber security infrastructure, practices, and systems to protect you and your patients. To that end, Eye Care Leaders has deployed or enhanced on its systems full-time, 24/7, multi-signal security monitoring, including threat hunting, end-to-end detection and blocking, and rapid containment and incident response. We have implemented additional patches and upgrades to older product versions to ensure they have up-to-date security, and we have taken proactive measures to enhance our network segmentation, system logging, authentication protocols, and firewall rules." Too little too late. And despite the significant outages that disrupted MVE users' practices and caused them damages, ECL again failed to reduce the monthly service fee for the outages as required under the MVE contracts.

108. Moreover, when Hofacre attempted to transition to a new EMR software provider due to ECL's failures, ECL failed to export Hofacre's patient data.

109. Upon information and belief, ECL Holdings, LLC, Eye Care Leaders Holdings, LLC, and Eye Care Leaders Portfolio Holdings, LLC participated in and orchestrated the aforementioned fraudulent conduct in concert with ECL.

VI. ECL's Revenue Cycle Management Failures and Breaches

110. ECL outsources its revenue cycle services to Alta Billing, LLC and Alta Billing Holdings, LLC.

111. Instead of improving the billing process for licensees' practices, ECL and the Alta entitieshad repeated problems.

112. Indeed, in February 2020, long before the ransomware attack, Alta Billing, LLC admitted to TEC that it had been sending bills under the wrong clinic's name. Specifically, Alta Billing, LLC continued to issue invoices under Reagan Eye Center, TEC's predecessor, despite having transitioned to sending out bills under TEC's name for months and having notice that Reagan Eye Center no longer existed.

113. Alta Billing, LLC even billed a surgery under the wrong surgeon. What is more, the operative report did not state that surgeon's name. Indeed, that surgeon had not performed a surgery in a year.

114. Despite its acknowledgement of wrongdoing, Alta Billing, LLC claimed that it could not correct the erroneous bills.

115. In the fall of 2020, Alta Billing, LLC again admitted that it had issued erroneous bills with the wrong provider, facility, and tax ID.

116. This time, Alta Billing, LLC had to conduct a claims audit to identify the scope of its errors.

117. In May 2021, Alta Billing, LLC admitted more failures. For the third time, Alta Billing, LLC sent incorrect statements without first obtaining TEC's authorization to

release the statements, even though some of the patients at issue were on a specific list of patients for which statements were not to be sent without prior approval by TEC.

118. Against TEC's billing policies of which Alta Billing, LLC was aware, Alta Billing, LLC also sent statements to self-pay patients.

119. In addition to these specific failures, Alta Billing, LLC simply failed to properly perform revenue cycle services and billing practices for the duration of the TEC contract.

120. Rather than streamline TEC's billing practices in a turn-key manner, TEC had to hire a new billing assistant and assign staff to review and revise Alta Billing, LLC's faulty work.

121. Ultimately, due to Alta Billing, LLC's repeated failures, TEC was forced to engage a new revenue cycle services vendor. That vendor has already uncovered at least $65,000 in unbilled or lost charges that Alta Billing, LLC should have billed.

122. Like TEC's experience, DRC, Hofacre, and other licensees also experienced repeated failures by Alta Billing, LLC to provide competent revenue cycle services that ECL agreed to provide.

123. In addition to its repeated mismanagement in breach of its agreement, ECL failed to disclose a ransomware attack it discovered on October 26, 2021 that created vulnerability in the online patient payment portal.

124. ECL agreed to maintain the security of the online patient payment portal through the use of industry-standard security protocols. Alta Billing, LLC and Alta Billing

Holdings, LLC were responsible for maintaining this security and using the industry-standard security protocols on ECL's behalf. ECL also agreed "to use appropriate safeguards, and comply with Subpart C of 45 C.F.R. Part 164 with respect to electronic [protected health information], to prevent use or disclosure of [protected health information] other than as provided for by the BAA, and "use appropriate administrative, physical, and technical safeguards to (a) maintain the security of the [protected health information] and (b) prevent the use and disclosure of [protected health information]." Again, Alta Billing, LLC and Alta Billing Holdings, LLC were responsible for using appropriate safeguards to prevent use or disclosure of information on ECL's behalf. Upon information and belief, Alta Billing, LLC and Alta Billing Holdings, LLC did not engage in the above safeguards and were negligent in maintaining the security of the online patient payment portal. This negligence resulted in the ransomware attack on October 26, 2021.

125. Even though ECL, Alta Billing, LLC, and Alta Billing Holdings, LLC were required to notify practices in the event of a breach of security, they intentionally hid this information from the practices.

126. On March 2, 2022—more than four months after discovering the vulnerability—ECL finally notified revenue cycle management clients that protected health information and personal identifying information were potentially compromised, including patient names, amount of payments, patient email addresses, and information in the comment section for the payment.

127. ECL, Alta Billing, LLC, and Alta Billing Holdings, LLC intentionally

omitted and concealed that the patient payment portal had suffered a ransomware attack creating a vulnerability that exposed patient information. They did so in an attempt to retain the licensees and to induce them to continue their revenue cycle management contracts. Licensees relied on the intentional omission and concealment by ECL to believe that no attack had occurred, that their patients' data had not been potentially compromised, that databases would be restored, and that they should continue their revenue cycle management contracts. As a result of ECL's, Alta Billing, LLC's, and Alta Billing Holdings, LLC's fraudulent omissions and licensees reasonable reliance on same, licensees suffered damages.

128. This also demonstrates yet another breach by ECL of its obligations under its agreements and BAAs to, among other things, "maintain the security of the [protected health information]" and "report promptly" to licensees "any use or disclosure of the [protected health information] not provided for by this BAA of which it becomes aware, including breaches of unsecured [protected health information], and any security incident of which it becomes aware."

129. ECL's, Alta Billing, LLC's, and Alta Billing Holdings, LLC's failure to protect transaction data and disclose this vulnerability until more than four months after its discovery has also caused revenue cycle management clients to suffer damages. The vulnerability created by the attack exposed, and therefore constitutes the written publication of, data in violation of the practices' and patients' right of privacy. Competitors could have accessed this data to identify the practices' lists of patients and also the rates

charged by the practices, which could lead to identification of the practices' agreements with insurers. Other bad actors could have accessed the data to use the payment information for their own gain via identity theft. ECL's, Alta Billing, LLC's, and Alta Billing Holdings, LLC's negligence violated the Revenue Cycle Management class's right of privacy and caused them damages in the form of (a) having to engage privacy professionals to ensure compliance with applicable laws, (b) having to research and determine whether their data had been compromised by exploitation of the vulnerability and written publication, (c) having to incur additional fees to transfer to a more reliable revenue cycle services vendor, (d) having to engage in additional security measures to protect their data; (e) having to spend additional resources to collect and manage payments from patients while the patient portal was compromised.

CLASS ALLEGATIONS

130. Plaintiffs bring this Class Action pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of themselves and others similarly situated.

131. Plaintiffs are representative of the following Proposed Class, which is divided into the following subclasses, defined as follows:

> **iMedicWare Class**: All persons and entities who contracted with ECL for EMR management services using the iMedicWare software, and who have suffered outages for any period of time since January 1, 2020, due to ransomware attacks or any other reasons.

myCare Integrity Class: All persons and entities who contracted with ECL—and received services from Integrity EMR, LLC and Integrity EMR Holdings, LLC—for EMR management services using the myCare Integrity software, and who have suffered outages for any period of time since January 1, 2020, due to ransomware attacks or any other reasons.

MVE Class: All persons and entities who contracted with ECL for EMR management services using the MVE software, and who have suffered outages for any period of time since January 1, 2020, due to ransomware attacks or any other reasons.

Revenue Cycle Management Class. All persons and entities who contracted with ECL—and received services from Alta Billing, LLC and Alta Billing Holdings, LLC—for revenue cycle management services who have received delinquent revenue cycle services for any period of time since January 1, 2020 and whose transaction information was potentially compromised from ransomware attacks or any other reasons.

132. Prosecution of the claims of the Proposed Class as a class action is appropriate because the prerequisites of Rule 23(a) of the Federal Rules of Civil Procedure are met:

- The number of persons in the Class is in the thousands, and the members of the Class are therefore so numerous that joinder of all members of the Class is impracticable. Joinder also is impracticable because of the geographic diversity of the members of the Class, and the need to expedite judicial relief.
- There are numerous questions of law and fact which are common to the members of the Class. These include, but are not limited to, common issues as to (1) whether ECL breached its obligations under its contracts with

members of the proposed class to provide EMR and revenue cycle management services; (2) whether all Defendants failed to use appropriate safeguards and otherwise protect the confidentiality and integrity of Plaintiffs' data and the protected health information stored on its servers; (3) whether all Defendants failed to disclose the ransomware attacks involving the Plaintiffs' data and instead issued misleading, fraudulent, and deceptive statements regarding the reasons for outages of the iMedicWare, myCare Integrity, and MVE software, and concealed the ransomware attack and vulnerability created in the online patient payment portal; (4) whether the conduct of all Defendants constitutes an unfair and deceptive trade practice; and (5) whether all Defendants were negligent.

133. The claims of the Named Plaintiffs are representative and typical of the claims of the Proposed Class and fairly encompass the claims of the Proposed Class. The Named Plaintiffs and Proposed Class are similarly situated and have been identically harmed by the same conduct on the part of Defendants.

134. The Named Plaintiffs and their counsel will fairly and adequately protect the interest of the Proposed Class. There are no material conflicts between the claims of the Named Plaintiffs and the members of the Proposed Class that would make class certification inappropriate. Counsel for the Proposed Class will vigorously assert the Proposed Class's claims.

135. In addition, the prosecution of the claims of the Proposed Class as a class

action pursuant to Rule 23(b)(3) is appropriate because:

- Questions of law or fact common to the members of the Proposed Class predominate over any questions affecting only its individual members; and
- A class action is superior to other methods for the fair and efficient resolution of the controversy.

136. The prosecution of the claims of the Proposed Class as a class action pursuant to Rule 23(b)(2) is appropriate because all Defendants have acted, or refused to act, on grounds generally applicable to the Proposed Class, thereby making appropriate final injunctive relief, or corresponding declaratory relief, for the Proposed Class as a whole.

CAUSES OF ACTION

FIRST CLAIM FOR RELIEF – BREACH OF CONTRACT (EMR Software – All Plaintiffs Against ECL)

137. The previous allegations are re-alleged and incorporated herein by reference.

138. The contracts between ECL and Alliance, TEC, DRC, Hofacre, and other entities are valid contracts.

139. By failing to maintain the security of Plaintiffs' data and access and functionality of the EMR software, as outlined herein, ECL breached the contracts.

140. Plaintiffs were damaged by ECL's breaches in excess of $75,000.

SECOND CLAIM FOR RELIEF – BREACH OF CONTRACT
(Revenue Cycle Services – TEC, DRC, Hofacre, and the Revenue Cycle Management Class Against ECL)

141. The previous allegations are re-alleged and incorporated herein by reference

142. By failing to provide competent revenue cycle services, as outlined herein, ECL breached the TEC contract and the DRC contract.

143. TEC and DRC were damaged by ECL's breaches.

THIRD CLAIM FOR RELIEF – BREACH OF CONTRACT
(BAAs – All Plaintiffs Against ECL)

144. The previous allegations are re-alleged and incorporated herein by reference.

145. The BAAs entered into between ECL and Plaintiffs are valid contracts.

146. As outlined herein, ECL breached the BAAs by failing to report promptly the security incidents and attacks that ECL experienced.

147. Plaintiffs were damaged by ECL's breaches.

FOURTH CLAIM FOR RELIEF – BREACH OF CONTRACT
(Failure to Provide Data – TEC, DRC, Hofacre Against ECL)

148. The previous allegations are re-alleged and incorporated herein by reference.

149. Even when a practice terminated its contract with ECL, ECL refused to comply with the provisions regarding the handling of the practice's data after termination.

150. Each contract expressly provided that if it was terminated, the respective practice could "export relevant patient data in CCDA (Consolidated Clinical Document Architecture) format" at no expense to the practice.

151. Yet ECL has failed and refuse to permit exportation of patient data.

152. Additionally, each contract provided that "upon prior written request from [the practice] in the event of termination," ECL would "(1) cooperate with [the practice] within reason, to transition Client Data to another EMR service provider using CCDA, and (2) prepare and deliver a secure file of all closed Clinic Notes in pdf format at ECL's standard hourly rates."

153. TEC, DRC, and Hofacre provided a written request to transition their data to a new EMR service provider. But ECL refused to cooperate with the practices to transition the data and failed to prepare and deliver a secure data file to the practices.

154. TEC, DRC, and Hofacre were damaged as a result of ECL's breaches.

155. Each practice is entitled to specific performance of its respective contract to obtain its data from ECL.

FIFTH CLAIM FOR RELIEF – FRAUD
(All Plaintiffs Against All Defendants)

156. The previous allegations are re-alleged and incorporated herein by reference.

157. That Defendants experienced attacks impacting the EMR software and online patient payment portal is a material fact.

158. Despite knowing it had experienced attacks causing the issues with the EMR software, ECL intentionally omitted and misrepresented that it had experienced an attack, instead telling Plaintiffs that it was experiencing mere "technical," "performance," and "system" issues.

159. With the intent to deceive Plaintiffs, ECL, Alta Billing, LLC, and Alta

Billing Holdings, LLC also intentionally omitted and concealed for months from TEC, DRC and the Revenue Cycle Management Class that ECL's online patient payment portal had suffered an attack that created a vulnerability exposing patient data in an effort to induce Plaintiffs to continue their contractual relationship with ECL.

160. Defendants omitted for a substantial period of time the true nature of the cause of the software issues.

161. Defendants intended to and did, in fact, deceive Plaintiffs about the cause of the software issues.

162. Defendants also knew after each attack that full functionality and access to its EMR software may not be restored for at least a month.

163. ECL, however, omitted this information from its communications with Plaintiffs about the duration of the software issues to hinder Plaintiffs and their other clients from exercising their rights under their EMR contracts or otherwise seeking to terminate the contracts due to ECL's breach and failure to comply with its obligations.

164. ECL instead informed Plaintiffs that it expected to correct the software issues soon.

165. Defendants intended to and did, in fact, deceive Plaintiffs about the duration of the software issues.

166. ECL also misrepresented to iMedicWare licensees that no data had been compromised or lost when, at the time of that misrepresentation, ECL knew that data from March 15-19, 2021 had been lost and was never recovered.

167. Defendants intended to and did, in fact, deceive iMedicWare licensees about the impact of the attack on its data in an effort to induce licensees to continue their contractual relationship with ECL.

168. Upon information and belief, ECL Holdings, LLC, Eye Care Leaders Holdings, LLC, Eye Care Leaders Portfolio Holdings, LLC, Integrity EMR, LLC, and Integrity EMR Holdings, LLC, Alta Billing, LLC, and Alta Billing Holdings, LLC participated in and orchestrated the aforementioned fraudulent conduct in concert with ECL.

169. Defendants controlled all information related to the attacks and the impact of same.

170. Plaintiffs had no way of independently verifying any information provided by Defendants, or obtaining information about the attacks and the impact of same from a different source.

171. Plaintiffs therefore reasonably relied on the information provided by Defendants. Plaintiffs reasonably relied on Defendants' omissions and false statements by not moving to a new vendor, hiring temporary staff to manually keep records in the meantime, and other actions.

172. Plaintiffs' reliance on Defendants' misrepresentations and material omissions caused Plaintiffs to suffer damages in excess of $75,000.

SIXTH CLAIM FOR RELIEF – NEGLIGENCE
(DRC and myCare Integrity Class Against ECL, ECL Holdings, LLC, Eye Care Leaders Holdings, LLC, Eye Care Leaders Portfolio Holdings, LLC)

173. The previous allegations are re-alleged and incorporated herein by reference.

174. ECL, ECL Holdings, LLC, Eye Care Leaders Holdings, LLC, Eye Care Leaders Portfolio Holdings, LLC owed a duty of care to DRC and the myCare Integrity class.

175. ECL, ECL Holdings, LLC, Eye Care Leaders Holdings, LLC, Eye Care Leaders Portfolio Holdings, LLC owed a duty to protect the privacy rights of DRC, the myCare Integrity class, and their patients.

176. ECL, ECL Holdings, LLC, Eye Care Leaders Holdings, LLC, Eye Care Leaders Portfolio Holdings, LLC breached this duty by, among other things, negligently failing to supervise its employees, failing to develop and implement reasonable and necessary policies to protect against malicious actions by its employees, and failing revoke an employee's software access credentials.

177. The negligence of ECL, ECL Holdings, LLC, Eye Care Leaders Holdings, LLC, Eye Care Leaders Portfolio Holdings, LLC proximately caused a violation of the right of privacy of DRC, the myCare Integrity class, and their patients due to creation of a vulnerability—written publication—of payment data.

178. DRC and the myCare Integrity class suffered damages in excess of $75,000 due to this negligence.

179. This duty of care and negligence is distinct from any contractual obligation

ECL Group, LLC owed DRC and the myCare Integrity class, and the damages are distinct from DRC's and the myCare Integrity class's damages sought under their fraud and breach of contract claims.

SEVENTH CLAIM FOR RELIEF – NEGLIGENCE
(DRC and myCare Integrity Class Against Integrity EMR, LLC and Integrity EMR Holdings, LLC)

180. The previous allegations are re-alleged and incorporated herein by reference.

181. Integrity EMR, LLC and Integrity EMR Holdings, LLC owed a duty to DRC and all other users of myCare Integrity to maintain the security of the software and their data.

182. Integrity EMR, LLC and Integrity EMR Holdings, LLC breached their duty of care to DRC and all other users of myCare Integrity.

183. Indeed, Integrity EMR, LLC and Integrity EMR Holdings, LLC failed to use industry-standard data security protocols, and other methods reasonably deemed to be adequate for secure business data. They also failed to "retain [patient] data on a secure server and to maintain data recovery and data backup facilities in accordance with accepted industry practices."

184. Integrity EMR, LLC's and Integrity EMR Holdings, LLC's negligence caused DRC and other users of myCare Integrity to suffer damages in excess of $75,000.

EIGHTH CLAIM FOR RELIEF – NEGLIGENCE
(TEC, DRC and Revenue Cycle Management Class Against ECL, ECL Holdings, LLC, Eye Care Leaders Holdings, LLC, Eye Care Leaders Portfolio Holdings, LLC)

185. The previous allegations are re-alleged and incorporated herein by reference.

186. ECL, ECL Holdings, LLC, Eye Care Leaders Holdings, LLC, Eye Care Leaders Portfolio Holdings, LLC owed a duty of care to TEC, DRC and the Revenue Cycle Management class.

187. ECL, ECL Holdings, LLC, Eye Care Leaders Holdings, LLC, Eye Care Leaders Portfolio Holdings, LLC owed a duty to protect the privacy rights of TEC, DRC, the Revenue Cycle Management class, and their patients.

188. ECL, ECL Holdings, LLC, Eye Care Leaders Holdings, LLC, Eye Care Leaders Portfolio Holdings, LLC breached this duty by, among other things, negligently failing to supervise its employees, failing to develop and implement reasonable and necessary policies to protect against malicious actions by its employees, and failing revoke an employee's software access credentials.

189. The negligence of ECL, ECL Holdings, LLC, Eye Care Leaders Holdings, LLC, Eye Care Leaders Portfolio Holdings, LLC proximately caused a violation of the right of privacy of TEC, DRC, the Revenue Cycle Management class, and their patients due to creation of a vulnerability—written publication—of payment data.

190. TEC, DRC and the Revenue Cycle Management class suffered damages in excess of $75,000 due to this negligence.

191. This duty of care and negligence is distinct from any contractual obligation ECL Group, LLC owed TEC, DRC, and the Revenue Cycle Management class, and the damages are distinct from TEC's, DRC's and the Revenue Cycle class's damages sought under their fraud and breach of contract claims.

NINTH CLAIM FOR RELIEF – NEGLIGENCE
(TEC, DRC, and Revenue Cycle Management Class Against Alta Billing, LLC and Alta Billing Holdings, LLC)

192. The previous allegations are re-alleged and incorporated herein by reference.

193. Alta Billing, LLC and Alta Billing Holdings, LLC owed a duty to TEC, DRC and the Revenue Cycle Management Class to maintain the security of the online patient payment portal and their data.

194. Alta Billing, LLC and Alta Billing Holdings, LLC breached their duty of care to TEC, DRC and the Revenue Cycle Management class.

195. Indeed, Alta Billing, LLC and Alta Billing Holdings, LLC failed to use industry-standard data security protocols, and other methods reasonably deemed to be adequate for secure business data.

196. Alta Billing, LLC's and Alta Billing Holdings, LLC's negligence caused TEC, DRC and the Revenue Cycle Management class to suffer damages in excess of $75,000.

TENTH CLAIM FOR RELIEF – DEFAMATION
(All Plaintiffs Against ECL)

197. The previous allegations are re-alleged and incorporated herein by reference.

198. ECL published false, defamatory statements about Plaintiffs to credit agencies, collection agencies, and others, stating that Plaintiffs had failed to pay amounts due under their contracts. Plaintiffs did not owe the amounts identified by ECL because the accounts had either been paid in full, or ECL had failed to reduce the fees as required due to the outages.

199. ECL's defamatory statements were defamatory both *per se* and *per quod* in that they impeached Plaintiffs in their trade and profession and as well as their creditworthiness.

200. Moreover, Plaintiffs are not public figures.

201. ECL's false and defamatory statements, even if only negligent, caused Plaintiffs damages in excess of $75,000.

ELEVENTH CLAIM FOR RELIEF - UNFAIR AND DECEPTIVE TRADE PRACTICES
(All Plaintiffs Against All Defendants)

202. The previous allegations are re-alleged and incorporated herein by reference.

203. Defendants' conduct related to the provision of EMR software is in or affecting commerce.

204. As outlined herein, Defendants engaged in fraudulent, deceptive, and other unfair acts to hide its failures and prevent, delay, or hinder Plaintiffs from switching EMR vendors.

205. For example, Defendants repeatedly stated one outage was the result of a "technical error" when it was in fact a ransomware attack. Defendants misrepresented

solutions to fix the outage and timeline for the same, when it knew those so-called solutions would not work, and, in any event, it could not and would not meet the deadlines it promised.

206. Indeed, Defendants actively concealed that it has suffered a ransomware attack. As an example, they hid the ransomware attack on the online patient payment portal for four months.

207. One of the reasons Defendants actively concealed its breaches was to deter further investigation.

208. Another purpose of Defendants' deceptive acts was to continue receiving the benefits of ECL's contracts, namely the payments it continued to bill for, and to dissuade the practices from terminating those contracts under their terms. While the other defendants did not contract directly with Plaintiffs, they were indirect beneficiaries of ECL's contracts with Plaintiffs and stood to gain by ensuring that the contractual relationships remained intact. Upon information and belief, all Defendants participated in and orchestrated the aforementioned fraudulent conduct in concert with ECL.

209. Furthermore, ECL's breaches of contract were accompanied by aggravating circumstances, such as misrepresentations, which amount to unfair and deceptive trade practices even where there is a contract between the parties.

210. Defendants' unfair and deceptive acts caused Plaintiffs to suffer damages in excess of $75,000.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray that the Court:

1. Trial by jury on all issues so triable;
2. Grant judgment in favor of Plaintiffs on all claims and order judgment for Plaintiffs in an amount of at least $75,000, trebled, and pre-judgment and post-judgment interest as allowed by law;
3. Award Plaintiffs their reasonable attorneys' fees under N.C. Gen. Stat. § 75-16.1;
4. Award Plaintiffs their reasonable costs and attorneys' fees as agreed in the contracts between ECL and Plaintiffs;
5. Tax the costs of this action against the Defendants;
6. Award specific performance, particularly regarding the return of Plaintiffs' data; and
7. Award such other and further relief as the Court may deem just or proper.

Respectfully submitted this the 1st day of May, 2023,

/s/ *Russ Ferguson*
Russ Ferguson (N.C. Bar No. 39671)
russ.ferguson@wbd-us.com
Matthew F. Tilley (NC Bar No. 40125)
matthew.tilley@wbd-us.com
Patrick G. Spaugh (N.C. Bar No. 49532)
patrick.spaugh@wbd-us.com

WOMBLE BOND DICKINSON (US) LLP
One Wells Fargo Center, Suite 3500
301 S. College Street
Charlotte, North Carolina 28202-6037
Phone: 704-331-4920