THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH
CAROLINA CASE NO: 1:22-CV-296

| | |
|---|---|
| ALLIANCE OPHTHALMOLOGY, PLLC; DALLAS RETINA CENTER, PLLC; AND TEXAS EYE AND CATARACT, PLLC, on behalf of themselves and all others similarly situated,<br><br>Plaintiffs,<br><br>v.<br><br>ECL GROUP, LLC,<br><br>Defendant. | **CLASS ACTION COMPLAINT** |

Plaintiffs, Alliance Ophthalmology, PLLC, Dallas Retina Center, PLLC, and Texas Eye and Cataract, PLLC, individually and on behalf a class of those similarly situated, complaining of ECL Group, LLC, allege as follows:

## 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 ("DRC") is a medical provider engaged in the practice of ophthalmology in Plano, Texas and Waxahachie, Texas.

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

4. ECL Group, LLC ("ECL") 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.

## JURISDICTION AND VENUE

5. This Court has personal jurisdiction over ECL because its principal place of business is located in this District.

6. 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.

7. 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.

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

9. 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

10. 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").

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

12. 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.

13. 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.

14. 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.

15. 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 and iMedicWare, 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.

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

17. Pursuant to those contracts, Alliance, TEC, DRC and other practices paid ECL both a one-time fee and monthly fee for their EMR software license.

18. 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.

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

(a) 1 hour if the issue was "loss or interruption of accessibility of the Software" due to ECL's failures;

(b) 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

(c) 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.

20. 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.

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

22. 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]

23. 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."

24. 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."

25. 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.

26. 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.

27. 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

[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).

information] and (b) prevent the use and disclosure of [protected health information]."

28. 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."

29. 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.

30. 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.

31. 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.

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

## III. ECL's iMedicWare Breach and Mismanagement.

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

34. 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 charts.

35. 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.

36. 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.

37. 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.

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

39. 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.

40. 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.

41. 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.

42. On March 26, 2021, nearly a week after the ransomware attack, ECL finally informed its licensees via mass email that iMedicWare had suffered a ransomware attack. ECL also admitted that some of its databases were corrupted or encrypted by the ransomware.

43. 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.

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

45. 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.

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

47. 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.

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

49. 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.

50. 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.

51. 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.

52. 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.

53. 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.

54. 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.

## IV. ECL's myCare Integrity Breach and Mismanagement.

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

56. 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.

57. ECL knew about the attack well before it informed licensees who used myCare Integrity.

58. Finally, on August 28, 2021, ECL informed licensees via a mass email that ECL had experienced an attack.

59. Upon information and belief, the attack was by a former ECL employee. After this employee stopped working for ECL, ECL failed to prohibit the employee from accessing ECL's systems. Thus, ECL's own former employee accessed its systems and wreaked havoc using the employee's prior credentials. This was not a sophisticated cyberattack; it was gross negligence.

60. 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."

61. ECL effectively hid from licensees that the widespread outages it was experiencing would last for weeks on end.

62. 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.

63. 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.

64. 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.

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

66. 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.

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

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

69. 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.

70. This breached ECL's obligations under the EMR contracts, under which ECL agreed to provide an export of patient data at no expense.

## V. ECL's Revenue Cycle Management Failures

71. ECL outsources its revenue cycle services to a third-party vendor, Alta Medical Management ("Alta").

72. Instead of improving the billing process for licensees' practices, ECL's vendor has had repeated problems.

73. Indeed, in February 2020, long before the ransomware attack, Alta admitted to TEC that it had been sending bills under the wrong clinic's name. Specifically, Alta 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.

74. Alta 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.

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

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

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

78. In May 2021, Alta admitted more failures. For the third time, Alta 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.

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

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

81. 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's faulty work.

82. Ultimately, due to Alta'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 should have billed.

83. DRC and other licensees, like TEC, also experienced repeated failures by Alta to provide competent revenue cycle services that ECL agreed to provide.

## CLASS ALLEGATIONS

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

85. 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 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.

**Revenue Cycle Management Class**. All persons who have contracted with ECL for revenue cycle management services who have received delinquent revenue cycle services for any period of time since January 1, 2020.

86. 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:

(a) 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.

(b) 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 ECL 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 ECL 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 and myCare Integrity software; and (4) whether ECL's conduct constitutes an unfair and deceptive trade practice.

87. 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 ECL.

88. 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.

89. In addition, the prosecution of the claims of the Proposed Class as a class action pursuant to Rule 23(b)(3) is appropriate because:

(a) Questions of law or fact common to the members of the Proposed Class predominate over any questions affecting only its individual members; and

(b) A class action is superior to other methods for the fair and efficient

resolution of the controversy.

90. The prosecution of the claims of the Proposed Class as a class action pursuant to Rule 23(b)(2) is appropriate because ECL has 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)

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

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

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

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

### SECOND CLAIM FOR RELIEF – BREACH OF CONTRACT (Revenue Cycle Services – TEC, DRC, and the Revenue Cycle Class)

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

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

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

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

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

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

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

101. Plaintiffs were damaged by ECL's breaches.

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

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

103. 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.

104. 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.

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

106. 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."

107. TEC and DRC 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.

108. TEC and DRC were damaged as a result of ECL's breaches.

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

**FIFTH CLAIM FOR RELIEF – FRAUD**
**(All Plaintiffs)**

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

111. That ECL experienced attacks impacting its EMR software is a material fact.

112. Despite knowing it had experienced attacks causing the issues with the EMR software, ECL informed Plaintiffs that it was experiencing mere "technical," "performance," and "system" issues.

113. ECL omitted for a substantial period of time the true nature of the cause of the software issues.

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

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

116. 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.

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

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

119. ECL controlled all information related to the attacks and the impact of same.

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

121. Plaintiffs therefore reasonably relied on the information provided by ECL—to whom Plaintiffs were paying substantial sums each month. Plaintiffs reasonably relied on ECL's omissions and false statements by not moving to a new vendor, hiring temporary staff to manually keep records in the meantime, and other actions.

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

**SIXTH CLAIM FOR RELIEF – UNFAIR AND DECEPTIVE TRADE PRACTICES**
**(All Plaintiffs)**

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

124. ECL's conduct related to the provision of EMR software is in or affecting commerce.

125. As outlined herein, ECL engaged in fraudulent, deceptive, and other unfair

acts to hide its failures and prevent, delay, or hinder Plaintiffs from switching EMR vendors.

126. For example, ECL repeatedly stated the outage was a "technical error" when it was in fact a ransomware attack. ECL 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.

127. Indeed, ECL actively concealed that it has suffered a ransomware attack.

128. One of the reasons ECL actively concealed its breaches was to deter further investigation.

129. Another purpose of ECL's deceptive acts was to continue receiving the benefits of its contracts, namely the payments it continued to bill for, and to dissuade the practices from terminating those contracts under their terms.

130. 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.

131. ECL's 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 Defendant;
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 15th day of April, 2022,

/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: 704-350-6361

# ClassAction.org