UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF MISSISSIPPI
OXFORD DIVISION

ADVANCED OBSTETRICS & GYNECOLOGY PC, individually, and on behalf of all others similarly situated, Plaintiff, vs. UNITEDHEALTH GROUP INCORPORATED, OPTUM, INC., and CHANGE HEALTHCARE INC., Defendants.	Case No. 3:24-CV-63-MPM-JVM **CLASS ACTION COMPLAINT** Jury Trial Demanded

Plaintiff Advanced Obstetrics & Gynecology PC ("Plaintiff" or "Advanced") brings this Class Action Complaint against Defendants UnitedHealth Group Incorporated ("United"), Optum, Inc. ("Optum"), and Change Healthcare Inc. ("Change") (collectively, "Defendants") based upon its personal knowledge, investigation by counsel, and review of public documents and states as follows:

INTRODUCTION

1. Plaintiff brings this action for Defendants' failure to timely and adequately process and pay the amounts due to medical providers for their services.

2. Change is a healthcare company that provides payment and revenue cycle services, clinical and imaging services, and other services to its clients. It is a lynchpin of a system which facilitates the payment of over $100 million per day to health care providers, many of which have limited liquidity.

3. Plaintiff seeks to hold Defendants responsible for the harms caused and will

continue to cause Plaintiff and other similarly situated persons in the massive and preventable cyberattack purportedly discovered by Defendants on February 21, 2024, in which cybercriminals, known as the BlackCat/ALPHV ransomware group, infiltrated Defendants' inadequately protected network and accessed highly sensitive information which was being kept unprotected ("Data Breach").

4. Indeed, Plaintiff and Class Members were wholly unaware of the Data Breach until they were unable to access important and sensitive information.

5. As a result of the breach, Change "disconnected [its] systems to prevent further impact," according to a statement it released on February 26, 2024. With those systems disconnected, Plaintiff and Class Members have been cut off from over 100 services provided by Change, including benefits verification, claims submission, and prior authorization. Without those services, Plaintiff and Class Members cannot be paid for their work with patients.

6. Defendants disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that sensitive information was safeguarded and failing to take available steps to prevent unauthorized disclosure of data and failing to follow applicable, required and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. Defendants further harmed Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently implementing procedures to disconnect the services that they rely on to secure payment. Plaintiff and Class Members are entitled to injunctive and other equitable relief.

PARTIES, JURISDICTION, AND VENUE

7. Plaintiff Advanced Obstetrics & Gynecology PC is a citizen of Mississippi. Its

principal place of business is located at 726 Coulter Drive, New Albany, MS 38652.

8. Defendant UnitedHealth Group Incorporated ("United") is a corporate citizen of Minnesota. It is a corporation with a principal place of business located at 9900 Bren Road East, Hopkins, Minnesota 55343-9664.

9. Defendant Optum, Inc. ("Optum") is a corporate citizen of Minnesota. It is a corporation with a principal place of business located at 11000 Optum Circle, Eden Prairie, Minnesota 55344. Optum is a subsidiary of United.

10. Defendant Change Healthcare Inc. ("Change") is a corporate citizen of Tennessee. It is a corporation with a principal place of business located at 424 Church Street, Suite 1400, Nashville, Tennessee 37219. Change is a subsidiary of Optum.

11. Jurisdiction is proper in this Court under 28 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendants.

12. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper in this Court under 28 U.S.C. § 1367.

13. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the events that gave rise to Plaintiff's claims took place within this District and Defendants conduct business in this Judicial District.

FACTUAL ALLEGATIONS

14. On February 21, 2024, Change failed to prevent a cyberattack affecting a number of its systems and services (the "Data Breach"). At 4:27 PM EST, it announced that it was "experiencing a network interruption related to a cyber security issue," that it had disconnected its

systems, and that disruption to its services was expected to last at least through the day. This disconnect has lasted at least 13 days and counting, with no resolution in sight. As a result of Change's failures, medical providers including Plaintiff and Class Members have been unable to receive payment for their services. As many Class Members, including Plaintiff, have limited liquidity, this disruption threatens to bankrupt hundreds if not thousands of care providers, if it hasn't done so already.

15. Change is a health software services company which provides payment and revenue cycle services, clinical imaging services, and other services to its clients. It is a large player in the healthcare sector, as its services allow health care providers to resolve payments for their care. It handles 15 billion healthcare transactions totaling more than $1.5 trillion annually. According to the Department of Justice, it handles 50 percent of all medical claims in the United States.

16. Plaintiff and Class Members are medical providers who have suffered delays in processing claims and revenue cycle services as a result of the Data Breach.

17. On March 4, 2024, The American Hospital Associations ("AHA") sent a letter to Congress stating:

> We are now on day 13 of this crisis and urgently need your support to help minimize further fallout from this attack.
>
> …
>
> Unfortunately, UnitedHealth Group's efforts to date have not been able to meaningfully mitigate the impact to our field. Workarounds to address prior authorization, as well as claims processing and payment are not universally available and, when they are, can be expensive, time consuming and inefficient to implement. For example, manually typing claims into unique payer portals or sending by fax machine requires additional hours and labor costs, and switching revenue cycle vendors requires hospitals and health systems to pay new vendor fees and can take months to implement properly.[1]

[1] *See* https://www.aha.org/lettercomment/2024-03-04-aha-urges-congress-provide-support-help-minimize-further-fallout-change-healthcare-attack.

18. In addition, the AHA explained to Congress that the funding assistance program United claims is helpful, is not:

> In addition, UnitedHealth Group's "Temporary Funding Assistance Program" that it stood up as part of its response on March 1 will not come close to meeting the needs of our members as they struggle to meet the financial demands of payroll, supplies and bond covenant requirements, among others.

Id.[2]

19. Given that it is a company in which half of America's medical payments flow, Change needs to maintain the utmost security of its systems. Indeed, Change states on its website that "[w]e implement and maintain organizational, technical, and administrative security measures designed to safeguard the data we process against unauthorized access, destruction, loss, alteration, or misuse."[3] As a sophisticated business entity, making promises that its systems were safe and secure, Change knew it needed to adequately protect those systems. It failed to do so.

20. According to reports, Change allowed its data and systems to be encrypted by the "Blackcat" ransomware gang, affiliated with AlphV. Ransomware attacks encrypt a target's computer systems in a manner that prevents the target from gaining access to their material, unless a ransom is paid in return for the passcode required to decrypt the system. It is a common form of cyberattack, and one that Change should have known it would be threatened with.

21. Defendant Change did not use reasonable security procedures and practices suited to the sensitive information they were maintaining. Worse, it compounded the attack by disconnecting all of its services, even though reports indicate that only certain systems were affected. By disconnecting all services, Change guaranteed that no medical providers could be

[2] https://www.optum.com/en/business/providers/health-systems/payments-lending-solutions/optum-pay/temporary-funding-assistance.html (explaining Temporary Funding Assistance Program for providers).
[3] https://www.changehealthcare.com/privacy-notice.

paid for their services.

22. Given the nature of the healthcare sector, many medical providers, like Advanced, are forced to rely on prompt payment of claims in order to keep their businesses alive. For instance, Advanced, over the past two years, has received approximately $39,000 in paid claims every week, meaning what Advanced receives weekly from insurance companies to settle the practice's bills for service. Advanced is unable to secure this payment due to Change's system lockout, and thus has been denied approximately $132,700 as of March 14, 2024, a figure that will continue to rise day after day. Had Change adequately secured its systems this large amount would have been timely paid, as Plaintiff had every reason to expect. has outstanding bills thus far totaling approximately $101,500.

CLASS ACTION ALLEGATIONS

23. Plaintiff brings this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure on behalf of Plaintiff and the following "Class:"

> All medical providers within the United States of America who have suffered delays in processing claims and revenue cycle services as a result of the Data Breach reported by Defendants on February 21, 2024.

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

25. This action has been brought and may properly be maintained as a class action under Fed. R. Civ. P. 23 because there is a well-defined community of interest in the litigation and

membership of the proposed Class is readily ascertainable.

26. **Numerosity**: A class action is the only available method for the fair and efficient adjudication of this controversy. The members of the Class are so numerous that joinder of all members is impractical, if not impossible. Plaintiff is informed and believe and, on that basis, allege that the total number of Class Members is in the thousands of individuals. Membership in the Class will be determined by analysis of Defendants' records.

27. **Commonality**: Plaintiff and the Class Members share a community of interest in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including, but not necessarily limited to:

i. Whether Defendants knew or should have known of the susceptibility of their data security systems to a data breach;

ii. Whether Defendants' security procedures and practices to protect their systems were reasonable in light of the measures recommended by data security experts;

iii. Whether Defendants' failure to implement adequate data security measures allowed the Data Breach to occur;

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

v. Whether Defendants adequately, promptly and accurately informed Plaintiff and Class Members about the Date Breach;

vi. How and when Defendants actually learned of the Data Breach;

vii. Whether Defendants' conduct, including their failure to act, resulted in or was the proximate cause of the breach of their systems, resulting in losses;

viii. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

ix. Whether Defendants engaged in unfair, unlawful or deceptive practices;

x. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief

and/or an accounting is/are appropriate as a result of Defendants' wrongful conduct;

xi. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendants' wrongful conduct.

28. **Typicality**: Plaintiff's claims are typical of the claims of the Plaintiff Class. Plaintiff and all members of the Plaintiff Class sustained damages arising out of and caused by Defendants' common course of conduct in violation of law, as alleged herein.

29. **Adequacy of Representation**: Plaintiff in this class action is an adequate representative of each of the Plaintiff Class in that Plaintiff have the same interest in the litigation of this case as the Class Members, are committed to the vigorous prosecution of this case and have retained competent counsel who are experienced in conducting litigation of this nature. Plaintiff is not subject to any individual defenses unique from those conceivably applicable to other Class Members or the Class in their entirety. Plaintiff anticipates no management difficulties in this litigation.

30. **Superiority**: The damages suffered by individual Class Members are significant but may be small relative to each member's enormous expense of individual litigation. This makes or may make it impractical for members of the Plaintiff Class to seek redress individually for the wrongful conduct alleged herein. Even if Class Members could afford such individual litigation, the court system could not. Should separate actions be brought or be required to be brought by each individual member of the Plaintiff Class, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants. The prosecution of separate actions would also create a risk of inconsistent rulings which might be dispositive of the interests of other Class Members who are not parties to the adjudications and/or may substantially impede their ability to protect their interests adequately. Individualized litigation increases the delay and expense to all

parties and to the court system, presented by the case's complex legal and factual issues. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale and comprehensive supervision by a single court.

31. Class certification is proper because the questions raised by this Complaint are of common or general interest affecting numerous persons, so it is impracticable to bring all Class Members before the Court.

32. This class action is also appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate concerning the Class in their entireties. Defendants' policies and practices challenged herein apply to and affect Class Members uniformly. Plaintiff's challenge of these policies and procedures hinges on Defendants' conduct concerning the Class in their entirety, not on facts or law applicable only to Plaintiff.

33. Unless a Class-wide injunction is issued, Defendants may continue failing to secure Class Members' PHI/PII properly, and Defendants may continue to act unlawfully, as set forth in this Complaint.

34. Further, Defendants have acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Fed. R. Civ. P. 23(b)(2).

CLAIMS FOR RELIEF

COUNT I
Negligence

35. Plaintiff realleges the allegations above as if fully set forth herein.

36. At all times herein relevant, Defendants owed Plaintiff and Class Members a duty

of care, *inter alia*, to act with reasonable care to secure and safeguard **that their claims and** revenue cycle services **would be processed on time and for the correct amounts.** Defendants took on this obligation and used their computer systems and networks to ensure that proper payments of claims were to be made.

37. Among these duties, Defendants were expected to provide claims processing and revenue cycle services to Plaintiff using safe and secure computer systems and networks.

38. Defendants owed a duty of care to not subject Plaintiff and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

39. Defendants knew or should have known of the vulnerabilities of their data security systems and the importance of adequate security. Defendants knew or should have known about numerous well-publicized data breaches.

40. Defendants knew or should have known that their data systems and networks did not adequately safeguard the claims processing and revenue cycle services.

41. Only Defendants were in the position to ensure that their systems and protocols were sufficient to protect Plaintiff and Class Members information.

42. Defendants breached their duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the claims processing and revenue cycle services.

43. Because Defendants knew that a breach of their systems could damage numerous individuals, including Plaintiff and Class Members, Defendants had a duty to adequately protect their data systems.

44. Plaintiff's and Class Members' willingness to entrust Defendants with their

processing needs was predicated on the understanding that Defendants would take adequate security precautions.

45. Defendants also had independent duties under state and federal laws that required Defendants to reasonably safeguard Plaintiff's and Class Members' PHI/PII and promptly notify them about the Data Breach.

46. Defendants' willful failure to abide by their duties was wrongful, reckless and/or grossly negligent in light of the foreseeable risks and known threats.

47. As a proximate and foreseeable result of Defendants' grossly negligent conduct, Plaintiff and Class Members have suffered damages and are at imminent risk of additional harm and damages.

48. The law further imposes an affirmative duty on Defendants to timely disclose the unauthorized access and failure to be able to process claims corrected or timely.

49. Further, explicitly failing to provide timely and clear notification of the Data Breach to Plaintiff and Class Members, Defendants prevented Plaintiff and Class Members from taking meaningful, proactive steps to secure processing needs which caused damages to Plaintiff.

50. There is a close causal connection between Defendants' failure to implement security measures to protect Plaintiff's and Class Members' processing requirements.

51. Defendants' wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

52. The damages Plaintiff and Class Members have suffered (as alleged above) and will continue to suffer were and are the direct and proximate result of Defendants' grossly negligent conduct.

53. Additionally, 15 U.S.C. § 45 (FTC Act, Section 5) prohibits "unfair […] practices

in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect private information like the processing of confidential claims. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

54. Defendants violated 15 U.S.C. § 45 by failing to use reasonable measures and by not complying with applicable industry standards, as described in detail herein.

COUNT II

Breach of Confidence

55. Plaintiff realleges the allegations above as if fully set forth herein.

56. During Plaintiff's and Class Members' interactions with Defendants, Defendants were fully aware of the important and confidential nature of the processing materials that Plaintiff and Class Members provided to them.

57. As alleged herein and above, Defendants' relationship with Plaintiff and Class Members was governed by promises and expectations that Plaintiff and Class Members' claims processing and revenue cycle service materials would be kept in confidence, and would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third-parties.

58. Plaintiff and Class Members provided their respective claims processing and revenue cycle services to Defendants with the explicit and implicit understandings that Defendants would protect and not permit the materials to be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third-parties.

59. Plaintiff and Class Members also provided their claims processing and revenue cycle service materials to Defendants with the explicit and implicit understanding that Defendants

would take precautions to protect those materials from unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing, such as following basic principles of protecting their networks and data systems and make ensure that claim payments related to the materials would be promptly paid and satisfied.

60. Due to Defendants' failure to prevent, detect and avoid the Data Breach from occurring by, *inter alia*, not following best information security practices to secure Plaintiff's and Class Members' claim processing, Plaintiff's and Class Members' materials were encumbered by and, not able to be used by Plaintiff in the manner expected.

61. As a direct and proximate cause of Defendants' actions and/or omissions, Plaintiff and Class Members have suffered damages, as alleged herein.

62. But for Defendants' failure to maintain and protect Plaintiff's and Class claims processing and revenue cycle services materials in violation of the parties' understanding of confidence, their materials would not have been accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third-parties.

63. The injury and harm Plaintiff and Class Members suffered and will continue to suffer was the reasonably foreseeable result of Defendants' unauthorized misuse of Plaintiff's and Class Members' materials. Defendants knew their data systems and protocols for accepting and securing Plaintiff's and Class Members' materials had security and other vulnerabilities that placed Plaintiff's and Class Members' materials in jeopardy.

COUNT III

Breach of Implied Contract

64. Plaintiff realleges the allegations above as if fully set forth herein.

65. Through their course of conduct, Defendants, Plaintiff and Class Members entered

into implied contracts for Defendants to implement data security and data processing functions adequate to safeguard and protect Plaintiff's and Class Members' claims processing and revenue cycle services materials.

66. Defendants required Plaintiff and Class Members to provide and entrust their claims processing and revenue cycle services materials as a condition of obtaining Defendants' services.

67. Defendants solicited and invited Plaintiff and Class Members to provide their claims processing and revenue cycle service materials as part of Defendants' regular business practices. Plaintiff and Class Members accepted Defendants' offers and provided their claim processing materials to Defendant.

68. Plaintiff and Class Members provided and entrusted their claims processing and revenue cycle services materials to Defendant. In so doing, Plaintiff and Class Members entered into implied contracts with Defendants by which Defendants agreed to ensure that Plaintiffs processing materials would not be defective or compromised.

69. A meeting of the minds occurred when Plaintiff and Class Members agreed to, and did, provide their claims processing and revenue cycle services materials to Defendant, in exchange for, amongst other things, the protection of their materials.

70. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

71. Defendants' breaches caused economic and non-economic harm.

COUNT IV

Breach of the Implied Covenant of Good Faith and Fair Dealing

72. Plaintiff realleges the allegations above as if fully set forth herein.

73. Contracts have an implied covenant of good faith and fair dealing. This implied

covenant is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

74. Plaintiff and Class Members have complied with and performed all conditions of their contracts with Defendants.

75. Defendants breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices and to process claims and services in a timely and safe manner as a result of the Data Breach.

76. Defendants knew or should have known of the vulnerabilities of the systems that were exploited in the Data Breach.

77. Defendants acted in bad faith and/or with malicious motive in denying Plaintiff and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

COUNT V

Breach of Fiduciary Duty

78. Plaintiff realleges the allegations above as if fully set forth herein.

79. In light of the special relationship between Defendants and Plaintiff and Class Members, whereby Defendants became the guardian of Plaintiff's and Class Members' claim processing materials, Defendants became a fiduciary by their undertaking and guardianship of the materials to act primarily for Plaintiff and Class Members.

80. Defendants have a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship with Class Members—in particular, to keep their claims processing and revenue cycle service materials secure.

81. Defendants breached their fiduciary duties to Plaintiff and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and

practicable period of time.

82. Defendants breached their fiduciary duties to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' claims processing and revenue cycle service materials.

83. Defendants breached their fiduciary duties to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

84. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer injuries.

COUNT VI

Unjust Enrichment

85. Plaintiff realleges the allegations above as if fully set forth herein. This Count is pled in the alternative to the Breach of Contract Count above.

86. Upon information and belief, Defendants fund their data-security measures entirely from their general revenue, including payments made by or on behalf of Plaintiff and Class Members.

87. As such, a portion of the payments made by or on behalf of Plaintiff and Class Members is to be used to provide a reasonable level of data security, and the amount of each payment allocated to data security is known to Defendants.

88. Plaintiff and Class Members conferred a monetary benefit to Defendant. Specifically, they purchased goods and services from Defendants and/or their agents and provided Defendants with their claims processing and revenue cycle service materials. In exchange, Plaintiff and Class Members should have received from Defendants the goods and services that were the subject of the transaction and have their processing and service materials protected with adequate data security.

89. Defendants knew that Plaintiff and Class Members conferred a benefit which Defendants accepted. Defendants profited from these transactions and used the claims processing and revenue cycle service materials of Plaintiff and Class Members for business purposes.

90. Defendants enriched themselves by saving the costs it reasonably should have expended in data-security measures to secure Plaintiff's and Class Members' claims processing materials. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendants instead calculated to increase their own profits at the expense of Plaintiff and Class Members.

91. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendants failed to implement appropriate data management and security measures mandated by industry standards.

92. If Plaintiff and Class Members knew that Defendants had not reasonably secured their claims processing materials, they would not have agreed to provide their PHI/PII to Defendants.

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

94. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendants' services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, and each member of the proposed Class respectfully requests that the Court enter judgment in their favor and for the following specific relief against Defendants as

follows:

1. That the Court declare, adjudge, and decree that this action is a proper class action and certify each of the proposed Class and/or any other appropriate Class under Fed. R. Civ. P. 23 (b)(1), (b)(2), and/or (b)(3), including the appointment of Plaintiff's counsel as Class Counsel;

2. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

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

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

5. For injunctive relief requested by Plaintiff, including but not limited to injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members;

6. For prejudgment interest on all amounts awarded, at the prevailing legal rate;

7. For an award of attorney's fees, costs, and litigation expenses, as allowed by law; and

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

JURY DEMAND

Plaintiff, individually and on behalf of the Class, hereby demands a trial by jury for all issues triable by jury.

Dated: March 14, 2024.

Respectfully submitted,

/s/ *Don Barrett*
John W. ("Don") Barrett

BARRETT LAW GROUP, P.A.
404 Court Square N
P.O. Box 927
Lexington, MS 39095
Tel: (662) 834-2488
dbarrett@barrettlawgroup.com

Richard R. Barrett (MSB # 99108)
LAW OFFICES OF RICHARD R. BARRETT, PLLC
2086 Old Taylor Rd., Suite 1011
Oxford, MS 38655
Tel: (662) 380-5018
rrb@rrblawfirm.net

Charles J. LaDuca
Brendan Thompson
Christian Hudson
CUNEO GILBERT & LADUCA, LLP
4725 Wisconsin Avenue NW
Suite 200
Washington, DC 20016
Tel: (202) 789-3960
charlesl@cuneolaw.com
brendant@cuneolaw.com
chudson@cuneolaw.com

Attorneys for Plaintiff