

**UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF INDIANA
HAMMOND DIVISION**

STATE OF INDIANA EX REL. ROKITA,

Plaintiff,

v.

CAREPOINTE, P.C.,

Defendant.

Case No. 2:23-cv-328-PPS-JPK

CONSENT JUDGMENT AND ORDER

Plaintiff, Indiana Attorney General *ex rel.* Todd Rokita, as *parens patriae* for the residents of the State of Indiana (the “State”), by counsel, Deputy Attorney General Jennifer M. Van Dame, and Defendant, CarePointe, P.C. (“CarePointe”) (collectively, the “Parties”), have agreed to the Court’s entry of this Consent Judgment and Order (“Consent Judgment”) without trial or adjudication of any issue of fact or law.

This Consent Judgment resolves the Plaintiff’s investigation of the data breach described in the Complaint filed in this action regarding CarePointe’s compliance with the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat.1936, as amended by the Health Information Technology for Economic and Clinical Health Act of 2009, Pub. L. No. 111-5, 123 Stat. 226, and

Department of Health and Human Services Regulations, 45 C.F.R. § 160, *et seq.* (collectively, “HIPAA”), as well as the Indiana Disclosure of Security Breach Act, Ind. Code § 24-4.9 *et seq.* (“DSBA”) and Indiana Deceptive Consumer Sales Act, Ind. Code § 24-5-0.5 *et seq.* (“DCSA”) (collectively, the “Relevant Laws”).

This Consent Judgment is not intended and shall not be used or construed as an admission by Defendant of any violation of the Relevant Laws, nor shall it be construed as an abandonment by the State of its allegations that Defendant violated the Relevant Laws.

The Parties consent to entry of this Consent Judgment by the Court as a final determination and resolution of the issues alleged in the Complaint.

THE PARTIES

1. The Office of the Indiana Attorney General (“OAG”) is charged with enforcement of the Relevant Laws, including HIPAA pursuant to 42 U.S.C. § 1320d-5(d).

2. CarePointe, P.C. (“CarePointe”) is an Indiana Professional Corporation with a principal office located at 99 E 86th Ave, Suite A, Merrillville, IN 46410.

BACKGROUND

3. On or around June 25, 2021, CarePointe was the target of a ransomware attack that exposed the Personal Information and/or Protected Health Information of approximately 45,002 Indiana residents.

4. The OAG investigated this incident pursuant to the Relevant Laws.

STIPULATIONS

5. The Parties agree to and do not contest the entry of this Consent Judgment.

6. At all times relevant to this matter, CarePointe was engaged in trade and commerce affecting consumers in the State of Indiana insofar as CarePointe provided health care services to consumers in Indiana. CarePointe was also in possession of the Personal Information and Protected Health Information of Indiana residents.

7. At all times relevant to this matter, CarePointe was a Covered Entity subject to the requirements of HIPAA.

8. The Parties consent to jurisdiction and venue in this Court for purposes of entry of this Consent Judgment as well as for the purpose of any subsequent action to enforce it.

JURISDICTION

9. The Court finds that it has jurisdiction over the Parties for purposes of entry of this Consent Judgment as well as for the purpose of any subsequent action to enforce it.

10. The Court finds that it has jurisdiction over the subject matter of this Consent Judgment pursuant to 42 U.S.C. § 1320d-5(d), 28 U.S.C. § 1331, and 28 U.S.C. § 1367 for the purpose of entering and enforcing the Consent Judgment, and venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(1). Further, the Court retains jurisdiction for the purpose of enabling the Parties to later apply to the Court

for such further orders and relief as may be necessary for the construction, enforcement, execution or satisfaction of this Consent Judgment.

ORDER

NOW THEREFORE, the Court has reviewed the terms of this Consent Judgment and based upon the Parties' agreement and for good cause shown, IT IS HEREBY ORDERED, ADJUDGED, AND DECREED AS FOLLOWS:

DEFINITIONS

11. For the purposes of this Consent Judgment, the following definitions shall apply:

- a. "Administrative Safeguards" shall be defined in accordance with 45 C.F.R. § 164.304 and are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect Electronic Protected Health Information and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information.
- b. "Breach" shall be defined in accordance with 45 C.F.R. § 164.402 to mean "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."
- c. "Business Associate" shall be defined in accordance with 45 C.F.R. §

160.103 and is a person or entity that provides certain services to or performs functions on behalf of covered entities, or other business associates of covered entities, that require access to Protected Health Information.

- d. “Covered Entity” shall be defined in accordance with 45 C.F.R. § 160.103 and is a health care clearinghouse, health plan, or health care provider that transmits health information in electronic form in connection with a transaction for which the U.S. Department of Health and Human Services has adopted standards.
- e. “DCSA” means the Indiana Deceptive Consumer Sales Act, Ind. Code § 24-5-0.5 *et seq.*, and any related statutes and rules adopted pursuant thereto. The DCSA is incorporated fully herein including all terms and definitions set forth therein.
- f. “DSBA” means the Indiana Disclosure of Security Breach Act, Ind. Code § 24-4.9 *et seq.*, and any related statutes and rules adopted pursuant thereto. The DSBA is incorporated fully herein including all terms and definitions set forth therein.
- g. “Effective Date” shall mean the date on which this Consent Judgment is approved by the Court.
- h. “Electronic Protected Health Information” or “ePHI” shall be defined in accordance with 45 C.F.R. § 160.103.
- i. “Encrypt” or “Encryption” shall mean to render unreadable,

indecipherable, or unusable to an unauthorized person through a security technology or methodology accepted generally in the field of information security.

- j. “HIPAA” means the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat.1936, as amended by the Health Information Technology for Economic and Clinical Health Act of 2009, Pub. L. No. 111-5, 123 Stat. 226, and any related Department of Health and Human Services Regulations, 45 C.F.R. § 160, *et seq.* HIPAA is incorporated fully herein including all terms and definitions set forth therein.
- k. “Minimum Necessary Standard” shall refer to the requirements of the Privacy Rule that, when using or disclosing Protected Health Information or when requesting Protected Health Information from another Covered Entity or Business Associate, a Covered Entity or Business Associate must make reasonable efforts to limit Protected Health Information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request as defined in 45 C.F.R. § 164.502(b) and § 164.514(d).
- l. “Personal Information” or “PI” shall be defined in accordance with Ind. Code § 24-4.9-2-10.
- m. “Privacy Rule” shall refer to the HIPAA Regulations that establish national standards to safeguard individuals’ medical records and other

Protected Health Information, including ePHI, that is created, received, used, or maintained by a Covered Entity or Business Associate that performs certain services on behalf of the Covered Entity, specifically 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and E.

- n. “Protected Health Information” or “PHI” shall be defined in accordance with 45 C.F.R. § 160.103.
- o. “Security Incident” shall be defined as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system in accordance with 45 C.F.R. § 164.304.
- p. “Security Rule” shall refer to the HIPAA Regulations that establish national standards to safeguard individuals’ Electronic Protected Health Information that is created, received, used, or maintained by a Covered Entity or Business Associate that performs certain services on behalf of the Covered Entity, specifically 45 C.F.R. Part 160 and 45 C.F.R. Part 164, Subparts A and C.
- q. “Technical Safeguards” shall be defined in accordance with 45 C.F.R. § 164.304 and means the technology and the policy and procedures for its use that protect Electronic Protected Health Information and control access to it.

INJUNCTIVE PROVISIONS

WHEREFORE, TO PROTECT CONSUMERS AND ENSURE FUTURE

COMPLIANCE WITH THE LAW:

Compliance with Federal and State Laws

8. Defendant shall comply with the HIPAA Privacy and Security Rules and shall implement all Administrative and Technical Safeguards required by HIPAA.

9. Defendant shall comply with DSBA and DCSA in connection with its collection, maintenance, and safeguarding of PI, PHI, and ePHI.

10. Defendant shall not make a misrepresentation which is capable of misleading consumers or fail to state a material fact if that failure is capable of misleading consumers regarding the extent to which Defendant maintains and/or protects the privacy, security, confidentiality, or integrity of PI, PHI, or ePHI.

Information Security Program

11. Overview: Within one hundred and twenty (120) days after the Effective Date, Defendant shall develop, implement, and maintain a written information security program (“Information Security Program” or “WISP”) that shall contain administrative, technical, and physical safeguards appropriate to: (i) the size and complexity of Defendant’s operations; (ii) the nature and scope of Defendant’s activities; and (iii) the sensitivity of the information that Defendant maintains. At a minimum, the WISP shall include the Specific Technical Safeguards and Controls in Paragraphs 17 through 28 below. Defendant may satisfy the requirements to implement and maintain the WISP through review, maintenance, and as necessary, updating of an existing information security program and related safeguards, provided that such program and safeguards meet the requirements of this Consent

Judgment. Defendant shall provide the resources and support necessary to fully implement the WISP so that it functions as required and intended by this Consent Judgment.

12. Governance: Defendant shall designate an individual whose responsibility will be to implement, maintain, and monitor the WISP (hereinafter referred to as the “HIPAA Security Officer” or “HSO”). The HSO shall have appropriate training to oversee the WISP and shall regularly report to the executive management regarding the status of the WISP, the security risks faced by the Defendant, resources required for implementation of the WISP, and the security implications of Defendant’s business decisions. At a minimum, the HSO shall report to the executive management any future Security Incident within twenty-four (24) hours of discovery, and shall also provide a copy of the documented Security Incidents and their outcomes to the executive management as needed in accordance with 45 C.F.R. § 164.308(a)(6)(ii).

13. Incident Response Plan: Defendant shall implement and maintain a written incident response plan (“Plan”) to prepare for and respond to any future Breaches. Defendant shall review and update the Plan as necessary. At a minimum, the Plan shall provide for the following phases:

- a. Preparation;
- b. Detection and Analysis;
- c. Containment;
- d. Notification and Coordination with Law Enforcement;

- e. Eradication;
- f. Recovery;
- g. Consumer and Regulator Notification; and
- h. Post-Incident Analysis and Remediation.

14. Table-Top Exercises: Defendant shall conduct, at a minimum, appropriate incident response plan exercises, every 18 months, to test and assess its preparedness to respond to Security Incidents and Breaches.

15. Training: Within one hundred and twenty (120) days of the Effective Date, and at least annually thereafter, Defendant shall provide data security and privacy training to all personnel with access to PI, PHI, or ePHI. Defendant shall provide this training to any employees newly hired to, or transitioned into, a role with access to PI, PHI, or ePHI, within thirty (30) days of hire or transition. Such training shall be appropriate to employees' job responsibilities and functions. Defendant shall document the trainings and the date(s) upon which they were provided.

16. Business Associates: Defendant shall develop, implement, and maintain written policies and procedures related to Business Associates, which at a minimum:

- a. Designate an individual as responsible for ensuring that Defendant enters into a Business Associate agreement with each of its Business Associates, prior to disclosing PI, PHI, or ePHI to the Business Associates;
- b. Assess Defendant's current and future business relationships to determine whether the relationship involves a Business Associate;

- c. Ensure that Defendant is entering into Business Associate agreements with Business Associates prior to disclosing PI, PHI, or ePHI to the Business Associates; and
 - d. Ensure that Defendant is limiting disclosures of PI, PHI, or ePHI to the minimum amount necessary for the Business Associate to perform their duties.
17. Minimum Necessary Standard: Defendant shall design and update the WISP consistent with the Minimum Necessary Standard.

Specific Technical Safeguards and Controls

18. Password Management: Defendant shall implement and maintain password policies and procedures requiring the use of strong, complex passwords with reasonable password-rotation requirements and ensuring that stored passwords are protected from unauthorized access.

19. Account Management: Defendant shall implement and maintain policies and procedures to manage, and limit access to and use of, all accounts with access to PI or ePHI, including individual accounts, administrator accounts, service accounts, and vendor accounts. Defendant shall not permit use of shared accounts with access to PI or ePHI.

20. Access Controls: Defendant shall implement and maintain policies and procedures to ensure that access to PI and ePHI is granted under the principle of least privilege. Such policies and procedures shall further include a means to regularly review access and access levels of users and require removal of network and

remote access within three (3) business days of notification of termination for any employee or vendor whose relationship with CarePointe has ended.

21. Multi-Factor Authentication: Defendant shall require the use of appropriate multi-factor authentication for remote access to Defendant's systems.

22. Asset Inventory: Defendant shall regularly inventory and classify all assets that comprise Defendant's network. The asset inventory shall, at a minimum, identify: (a) the name of the asset; (b) the version of the asset; (c) the owner of the asset; (d) the asset's location within the network; (e) the asset's criticality rating; (f) whether the asset collects, processes, or stores PI or ePHI; and (g) each security update or patch applied or installed during the preceding period.

23. Vulnerability Scanning: Defendant shall conduct regular vulnerability scanning using industry-standard tool(s) and shall take appropriate steps to remediate identified vulnerabilities.

- a. Any critical or high-risk vulnerability that is associated with a Security Incident shall be remediated within forty-eight (48) hours of the identification of the vulnerability. If the vulnerability cannot be remediated as indicated above, then Defendant shall within forty-eight (48) hours of the identification of such vulnerability take the application or system affected by such vulnerability offline until such vulnerability is remediated.

24. Software Updates and Patch Management: Defendant shall implement and maintain a reasonable policy to update and patch software on its network.

Defendant shall employ processes and procedures to ensure the timely scheduling and installation of any security update or patch, considering (without limitation) the severity of the vulnerability for which the update or patch has been released to address, the severity of the issue in the context of the Defendant's network, the impact on Defendant's operations, and the risk ratings articulated by the relevant software and application vendors or disseminated by a U.S. government authority.

25. Segmentation: Defendant shall implement and maintain policies and procedures designed to appropriately segment its network, which shall, at a minimum, ensure that systems communicate with each other only to the extent necessary to perform their business and/or operational functions.

26. Encryption: Defendant shall Encrypt PI and ePHI at rest and in transit as appropriate, and in accordance with applicable law.

27. Logging and Monitoring: Defendant shall implement and maintain reasonable controls to centralize logging and monitoring of Defendant's network; to report anomalous activity through the use of appropriate platforms; and to require that tools used to perform these tasks be appropriately monitored and tested to assess proper configuration and maintenance. Defendant shall ensure that logs of system activity are regularly reviewed and analyzed, that logs are protected from unauthorized access or deletion, and that appropriate follow-up and remediation steps are taken with respect to any Security Incident.

28. Intrusion Detection and Prevention: Defendant shall implement and maintain intrusion detection and prevention tools, including but not limited to

firewalls and antivirus/antimalware software.

29. Penetration Testing: Defendant shall implement and maintain a risk-based penetration testing program reasonably designed to identify, assess, and remediate potential security vulnerabilities. Such testing shall occur at least every eighteen (18) months and shall include penetration testing of Defendant's internal and external network defenses. Defendant shall review the results of such testing, take steps to remediate findings revealed by such testing, and document such remediation. Defendant shall document the penetration test results and remedial measures, retain such documentation for six (6) years, and provide such documentation to the State upon request.

Assessment and Reporting Requirements

30. HIPAA Risk Analysis and Risk Management Plan: Defendant shall obtain an annual risk assessment by a qualified, independent third party, which shall, at a minimum, include: the identification of internal and external risks to the security, confidentiality, or integrity of PHI or ePHI that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information; an assessment of the safeguards in place to control these risks; an evaluation and adjustment of the WISP considering the results of the assessment, including the implementation of reasonable safeguards to control these risks; and documentation of safeguards implemented in response to such risk assessments. Defendant shall document the risk assessments and remedial measures, retain such documentation for six (6) years, and provide such documentation to the State upon

request.

31. Information Security Program Assessment: Defendant shall, within one hundred and eighty (180) days of the Effective Date, and thereafter biennially for a period of six (6) years, submit to an assessment of its compliance with this Consent Judgment by a qualified, independent third party (“Assessor”). Following each such assessment, the Assessor shall prepare a report including its findings and recommendations (“Security Report”), a copy of which shall be provided to the Indiana Attorney General within forty-five days (45) of its completion.

- a. Within one hundred and twenty (120) days of receipt of each Security Report, Defendant shall review and, to the extent necessary, revise its current policies and procedures based on the findings of the Security Report.
- b. Within one hundred eighty (180) days of Defendant’s receipt of each Security Report, Defendant shall forward to the Indiana Attorney General a description of any action Defendant takes and, if no action is taken, a detailed description why no action is necessary, in response to each Security Report.

Payment to the State

32. Within thirty (30) days of the Effective Date, Defendant shall pay One Hundred and Twenty-Five Thousand Dollars (\$125,000.00) to the Office of the Indiana Attorney General, to be used for any purpose allowable under Indiana law. For purposes of IRS Form 1098-F, all payments shall be reported in Box 2 as “Amount

to be paid for violation or potential violation.” To effectuate this payment and reporting, the State shall provide Defendant with an IRS Form W-9 and ACH instructions, and Defendant shall provide the State with an IRS Form W-9 upon execution of this Consent Judgment.

Release

33. Following full payment of the amount due by Defendant under this Consent Judgment, the State shall release and discharge Defendant from all civil claims that the State could have brought under the Relevant Laws, based on Defendant’s conduct as set forth in the Complaint. Nothing contained in this paragraph shall be construed to limit the ability of the State to enforce the obligations that Defendant or its officers, subsidiaries, affiliates, agents, representatives, employees, successors, and assigns have under this Consent Judgment. Further, nothing in the Consent Judgment shall be construed to create, waive, or limit any private right of action.

34. Notwithstanding any term of this Consent Judgment, any and all of the following forms of liability are specifically reserved and excluded from the release in Paragraph 33 above as to any entity or person, including Defendant:

- a. Any criminal liability that any person or entity, including Defendant, has or may have;
- b. Any civil liability or administrative liability that any person or entity, including Defendant, has or may have under any statute, regulation, or rule not expressly covered by the release in Paragraph 33 above,

including but not limited to, any and all of the following claims: (i) State or federal antitrust violations; (ii) State or federal securities violations; (iii) State insurance law violations; or (iv) State or federal tax claims.

Consequences of Noncompliance

35. Defendant represents that it has fully read this Consent Judgment and understands the legal consequences attendant to entering into this Consent Judgment. Defendant understands that any violation of this Consent Judgment may result in the State seeking all available relief to enforce this Consent Judgment, including an injunction, civil penalties, court and investigative costs, attorneys' fees, restitution, and any other relief provided by the laws of the State or authorized by a court. If the State is required to file a petition to enforce any provision of this Consent Judgment against Defendant, Defendant agrees to pay all court costs and reasonable attorneys' fees associated with any successful petition to enforce any provision of this Consent Judgment against such Defendant.

General Provisions

36. Any failure of the State to exercise any of its rights under this Consent Judgment shall not constitute a waiver of any rights hereunder.

37. Defendant hereby acknowledges that its undersigned representative or representatives are authorized to enter into and execute this Consent Judgment. Defendant is and has been represented by legal counsel and has been advised by its legal counsel of the meaning and legal effect of this Consent Judgment.

38. This Consent Judgment shall bind Defendant and its officers, subsidiaries, affiliates, agents, representatives, employees, successors, future purchasers, acquiring parties, and assigns.

39. Defendant shall deliver a copy of this Consent Judgment to its executive management having decision-making authority with respect to the subject matter of this Consent Judgment within thirty (30) days of the Effective Date.

40. The settlement negotiations resulting in this Consent Judgment have been undertaken by the Parties in good faith and for settlement purposes only, and no evidence of negotiations or communications underlying this Consent Judgment shall be offered or received in evidence in any action or proceeding for any purpose.

41. Defendant waives notice and service of process for any necessary filing relating to this Consent Judgment, and the Court retains jurisdiction over this Judgment and the Parties hereto for the purpose of enforcing and modifying this Consent Judgment and for the purpose of granting such additional relief as may be necessary and appropriate. No modification of the terms of this Consent Judgment shall be valid or binding unless made in writing, signed by the Parties, and approved by the Court in which the Consent Judgment is filed, and then only to the extent specifically set forth in such Consent Judgment. The Parties may agree in writing, through counsel, to an extension of any time period specified in this Consent Judgment without a court order.

42. Defendant does not object to *ex parte* submission and presentation of this Consent Judgment by the Plaintiff to the Court, and does not object to the Court's

approval of this Consent Judgment and entry of this Consent Judgment by the Clerk of the Court.

43. The Parties agree that this Consent Judgment does not constitute an approval by the State of any of Defendant's past or future practices, and Defendant shall not make any representation to the contrary.

44. The requirements of the Consent Judgment are in addition to, and not in lieu of, any other requirements of federal or state law. Nothing in this Consent Judgment shall be construed as relieving Defendant of the obligation to comply with all local, state, and federal laws, regulations, or rules, nor shall any of the provisions of the Consent Judgment be deemed as permission for Defendant to engage in any acts or practices prohibited by such laws, regulations, or rules.

45. This Consent Judgment shall not create a waiver or limit Defendant's legal rights, remedies, or defenses in any other action by the Plaintiff, except an action to enforce the terms of this Consent Judgment or to demonstrate that Defendant was on notice as to the allegations contained herein.

46. This Consent Judgment shall not waive Defendant's right to defend itself, or make argument in, any other matter, claim, or suit, including, but not limited to, any investigation or litigation relating to the subject matter or terms of the Consent Judgment, except with regard to an action by the Plaintiff to enforce the terms of this Consent Judgment.

47. This Consent Judgment shall not waive, release, or otherwise affect any claims, defenses, or position that Defendant may have in connection with any investigations, claims, or other matters not released in this Consent Judgment.

48. Defendant shall not participate directly or indirectly in any activity to form or proceed as a separate entity or corporation for the purpose of engaging in acts prohibited in this Consent Judgment or for any other purpose which would otherwise circumvent any part of this Consent Judgment.

49. If any clause, provision, or section of this Consent Judgment shall, for any reason, be held illegal, invalid, or unenforceable, such illegality, invalidity, or unenforceability shall not affect any other clause, provision, or section of this Consent Judgment and this Consent Judgment shall be construed and enforced as if such illegal, invalid, or unenforceable clause, section, or other provision had not been contained herein.

50. Unless otherwise prohibited by law, any signatures by the Parties required for entry of this Consent Judgment may be executed in counterparts, each of which shall be deemed an original, but all of which shall be considered one and the same Consent Judgment.

51. To the extent that there are any, Defendant agrees to pay all court costs associated with the filing of this Consent Judgment.

52. The orders contained in this Consent Judgment shall be effective for six (6) years following the Effective Date.

Notices

53. Any notices or other documents required to be sent to the Parties pursuant to the Consent Judgment shall be sent by (A) email; and (B) United States Mail, Certified Return Receipt Requested, or other nationally recognized courier service that provides tracking services and identification of the person signing for the documents. The required notices and/or documents shall be sent to:

a. For the State:

Douglas S. Swetnam
Section Chief – Data Privacy & Identity Theft Unit
Office of Attorney General Todd Rokita
302 West Washington Street
IGCS-5th Floor
Indianapolis, IN 46204
douglas.swetnam@atg.in.gov

Jennifer M. Van Dame
Deputy Attorney General
Office of Attorney General Todd Rokita
302 West Washington Street
IGCS-5th Floor
Indianapolis, IN 46204
jennifer.vandame@atg.in.gov

b. For Defendant:

Kevin Scott
Shareholder
Greenberg Traurig, LLP
77 W Wacker Dr
Suite 3100
Chicago, IL 60601
Kevin.scott@gtlaw.com

IT IS STIPULATED:

FOR THE STATE OF INDIANA


Office of Indiana Attorney General

By 

Date: 11/01/2023


Jennifer M. Van Dame
Attorney No. 32788-53
Deputy Attorney General
Office of the Indiana Attorney General
302 West Washington Street
Indianapolis, IN 46037

FOR DEFENDANT

By 

Date: 10/30/23

Dennis P. Han
Managing Partner
CarePointe, P.C.
99 East 86th Avenue, Suite A
Merriville, IN 46410

By 

Date: 30 October 2023

Kevin Scott
Shareholder
Greenberg Traurig, LLP
77 W Wacker Dr, Suite 3100
Chicago, IL 60601

SO ORDERED, ADJUDGED, AND DECREED:

By /s/ Philip P. Simon
JUDGE

Date: November 28, 2023