COMMONWEALTH OF MASSACHUSETTS

SUFFOLK, ss	SUPERIOR COURT CIVIL ACTION NO. 2684CV00265

COMMONWEALTH OF MASSACHUSETTS,

Plaintiff,

v.

COMSTAR, LLC,

Defendant.

[Proposed] FINAL JUDGMENT BY CONSENT

The Court has reviewed the Complaint in this matter filed by the Commonwealth of Massachusetts through the Attorney General's Office ("Commonwealth"), the Joint Motion for Entry of Final Judgment by Consent, and the attached Consent to Judgment. The Court finds that it has subject matter jurisdiction over this matter, and that the defendant Comstar, LLC. ("Comstar") has consented to specific personal jurisdiction in Massachusetts for purposes of this matter. The Court further finds that the entry of this Final Judgment by Consent ("Final Judgment") is in the interests of justice.

WHEREAS, the Attorney General is authorized to bring an action in this Court under G. L. c. 93H, § 6, and G. L. c. 93A, § 4. The Attorney General is also authorized to enforce the Health Insurance Portability and Accountability Act ("HIPAA") as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act, Pub. L. No. 111-5, 123 Stat. 226, 42 U.S.C. § 1320d-5(d).

WHEREAS, Defendant Comstar is a Massachusetts-based limited liability company that provides ambulance billing and collection services across the Northeast. Comstar's principal place of business is located at 8 Turcotte Memorial Drive, Rowley, MA 01960.

WHEREAS, Comstar discovered suspicious activity on its network on March 26, 2022, confirmed unauthorized access on April 21, 2022, and disclosed the incident to the Commonwealth and the Attorney General of Connecticut (collectively, "the States") on May 25, 2022 (the "Data Breach") which impacted approximately 22,829 Connecticut residents and 326,426 Massachusetts residents. The Data Breach compromised the "personal information" ("PI") as that term is defined in G.L. c. 93H, § 1 and "personal health information" ("PHI") as that term is defined in 45 C.F.R. § 160.130, including names, dates of birth, medical assessment and medication administration information, health insurance information, Social Security numbers and/or Medicare numbers.

WHEREAS, the States conducted and concluded an investigation into the circumstances surrounding the Data Breach Incidents and Comstar's policies, procedures, and practices regarding the security of PI. In particular, the States investigated Comstar's compliance with the Massachusetts Consumer Protection Act, G.L. c. 93A, the Massachusetts Data Security Law, G.L. c. 93H, the Massachusetts Data Security Regulations, 201 C.M.R. 17.00-17.05, and HIPAA.

WHEREAS, the Commonwealth, in the Complaint, alleges that Comstar violated G.L. c. 93A, G.L. c. 93H, the Massachusetts Data Security Regulations, 201 CMR 17.00-17.05., and HIPAA, found at 45 C.F.R. Part 164, Subparts A, C, and E.

WHEREAS, the Commonwealth acknowledges Comstar's cooperation with the States' investigation of this matter, including with respect to the negotiation of this Final Judgment.

WHEREAS, without acknowledging liability or culpability, in order to resolve their differences concerning this case, and in order to avoid the cost and uncertainty of litigation, the parties have agreed to entry of this Final Judgment.

WHEREAS, Defendant is entering into a Judgment with the Commonwealth of Massachusetts and the State of Connecticut and each respective Judgment incorporates the substantive terms included herein. To the extent there are differences, those differences are related to and/or arise from the requirements of local rules and state laws as well as the facts of the Data Breach.

WHEREAS, the parties have filed a joint motion seeking entry of this Final Judgment.

Accordingly, **IT IS HEREBY ORDERED AND ADJUDGED THAT:**

I. DEFINITIONS

1. "Consumer Protection Act" refers to G.L. c. 93A.

2. "Business Associate" shall be defined in accordance with 45 C.F.R. § 160.103 and refers to a person or entity that provides certain services for or performs functions on behalf of "Covered Entities," and requires access to Protected Health Information to provide such services or perform such functions..

3. "Covered Entity" or "Covered Entities" 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 United States Department of Health and Human Services has adopted standards**.**

4. "Data Breach Notification Law" refers to G.L. c. 93H § 3A.

5. "Effective Date" shall be the date of entry of this judgment.

6. “Encrypt” or “Encryption” shall mean to render data unreadable, indecipherable, or unusable to an unauthorized person through a security technology or methodology accepted generally in the field of information security commensurate with the sensitivity of the data at issue.

7. “HIPAA Privacy Rule” shall refer to the HIPAA Regulations that establish national standards to safeguard individuals’ medical records and other Protected Health Information as defined at 45 C.F.R. Parts 160 and subparts A and E of Part 164.

8. “HIPAA Security Rule” shall refer to the HIPAA regulations that establish national standards to safeguard individuals’ Electronic Protected Health Information as defined at 45 C.F.R. Parts 160 and subparts A and C of Part 164.

9. “Minimum Necessary Standard” shall refer to the requirements of the Privacy Rule as defined in 45 C.F.R. §§ 164.502(b) and 164.514(d).

10. “Multi-factor Authentication” shall mean user account authentication through verification of at least two of the following factors: (i) knowledge factors such as a password; or (ii) possession factors, such as a token, connection through a known authenticated source, or a text message on a mobile phone; or (iii) inherent factors, such as biometric characteristics.

11. “Personal Information” or “PI” shall have the same meaning as set forth in 201 C.M.R. § 17.02.

12. “Protected Health Information” or “PHI” is defined in accordance with 45 C.F.R. § 160.103.

13. “Personal Information Protection Act” refers to G.L. c. 93H, and the associated Data Security Regulations, 201 CMR 17.00-17.05.

14. “Security Event” refers to any compromise, or threat that gives rise to a reasonable likelihood of compromise to the confidentiality, integrity, or availability of PI and/or PHI of U.S.

consumers where such PI and PHI is collected, processed, transmitted, stored or disposed of by Comstar.

II. INJUNCTIVE RELIEF

15. Now therefore, on the basis of these findings and stipulations, the Defendant agrees to the relief below:

Compliance with State and Federal Laws

16. Comstar shall comply with the Consumer Protection Act, the Personal Information Protection Act, and the HIPAA Privacy and Security Rules in connection with its collection, maintenance, and safeguarding of PI and PHI.

17. Comstar shall not misrepresent the extent to which it maintains and/or protects the privacy, security, confidentiality, or integrity of PI or PHI.

18. Comstar shall comply with the reporting and notification requirements of the Data Breach Notification Law and Mass. G.L. c. 93H § 3.

Information Security Program

19. Comstar shall develop, implement, maintain, and comply with a comprehensive information security program ("Information Security Program" or "Program") that is reasonably designed to protect the security, integrity, and confidentiality of PI and PHI that Comstar collects, stores, transmits, maintains, and/or destroys in compliance with Massachusetts's requirements for a Written Information Security Program ("WISP") under 201 CMR 17.00 and Mass. G.L. c. 93H. The Information Security Program shall, at a minimum, include the specific information security safeguards set forth in Paragraphs 20 through 39 of this Judgment.

20. Comstar's Information Security Program shall be documented and must contain administrative, technical, and physical safeguards appropriate to (i) the size and complexity of

Comstar's operations; (ii) the nature and scope of Comstar's activities; and (iii) the sensitivity of the PI and PHI that Comstar collects, stores, transmits, maintains and/or destroys.

21. Comstar shall consider, and adopt where feasible, the principles of zero trust architecture in the design of the Information Security Program.

22. Comstar shall retain the services of an executive, officer, or vendor with appropriate background or experience who shall be responsible for advising the Chief Executive Officer and Designated Security Officer ("CEO") on implementing, maintaining, and monitoring the Program (hereinafter referred to as the Chief Information Security Officer or "CISO"). Comstar shall ensure that the role of the CISO shall include regular and direct reporting to the CEO on at least a semi-annual basis of Comstar's security posture and the security risks faced by Comstar. The CISO shall report Security Incidents to the CEO within twenty-four hours of discovery. The CEO shall be ultimately responsible for maintaining the Information Security Program.

23. Comstar shall, as part of the Information Security Program, implement and maintain a written incident response plan ("Plan") to prepare for and respond to Security Events. Comstar shall review this Plan annually, then revise and update the Plan as necessary to adapt to any material changes that affect the security of PI and PHI. At a minimum, this Plan shall provide for the following phases of a response: (i) Preparation; (ii) Detection and Analysis; (iii) Containment; (iv) Notification and Coordination with Law Enforcement; (v) Recovery; (iv) Consumer and Regulator Notification and Remediation; and (viii) Post-Incident Analysis.

24. Comstar shall provide notice of the requirements of this Judgment to its employees responsible for implementing, maintaining, or monitoring the Information Security Program, including by not limited to the CISO, within sixty (60) days of the Effective Date or prior to their responsibilities for implementing, maintaining, or monitoring the Information Security Program.

Comstar shall ensure that such employees have sufficient knowledge of the requirements of this Judgment and receive specialized training on safeguarding and protecting consumer Personal Information to help effectuate Comstar's compliance with the terms of this Judgment.

25. Comstar shall further incorporate security awareness and privacy training for all personnel who have access to PI or PHI, which training shall be appropriate to the employees' job responsibilities and functions. Within ninety (90) days of the Effective Date, Comstar shall confirm to the Attorneys General that such training has been provided, and thereafter, shall provide it to all such employees on at least an annual basis. Comstar must also develop accountability metrics to measure each participant's compliance with training requirements.

26. Comstar may satisfy the implementation and maintenance of the Information Security Program through review, maintenance, and as necessary, updating of an existing information security program or existing safeguards, provided that such program and safeguards meet the requirements of this Judgment.

27. Comstar shall provide the resources and support necessary to fully implement the Program so that it functions as required and intended by this Judgment.

Specific Information Security Requirements

28. **Minimum Necessary**: Comstar shall collect and/or maintain PI and PHI only to the extent necessary to accomplish its intended purpose and to fulfill its regulatory, legal, and contractual obligations. In accordance with the Minimum Necessary Standard requirements of the Privacy Rule, Comstar shall maintain no more than 2 years' worth of records in its live database. To the extent required by applicable law, Comstar will archive 2-7 year old records within its offline archive database. At a minimum, such archiving shall be performed on a quarterly basis.

29. **Access Controls**: Comstar shall implement and maintain appropriate policies and controls to manage access to and use of accounts with access to PI or PHI. Such policies shall at a minimum require that Comstar:

a. terminate access privileges for all persons whose access to the Comstar network is no longer required or appropriate.

b. limit access to Personal Information by persons accessing the Comstar network on a least-privileged basis.

c. regularly inventory the users who have access to the Comstar network in order to review and determine whether or not such access remains necessary or appropriate. Comstar shall regularly compare termination lists to user accounts to ensure access privileges have been appropriately terminated. At a minimum, such review shall be performed on a quarterly basis.

d. implement and maintain adequate processes and procedures to store and monitor the account credentials and access privileges of employees who have privileges to design, maintain, operate, and update the Comstar network.

e. Regular review account logins, account creations, and password rests for activity indicative of a data security incident (including, for example, a high number of failed login attempts).

30. **Password Management**: Comstar shall implement and maintain policies and procedures requiring the use of strong and complex passwords and password rotation, and ensuring that stored passwords are properly protected from unauthorized access. For purposes of the Paragraph:

a. any administrative-level passwords shall be Encrypted or secured using a password vault, privilege access monitoring, or an equal or greater security tool that is generally accepted by the security industry.

b. Comstar shall securely store passwords based on industry best practices; for example, hashing passwords stored online using an appropriate hashing algorithm that is not vulnerable to a collision attack together with an appropriate salting policy, or other equivalent or stronger protections.

31. **Multi-Factor Authentication**: Comstar shall require multi-factor authentication for all individual user accounts, including system administrator accounts, and for remote access to its computer network.

32. **Encryption:** Comstar shall implement and maintain policies and procedures to encrypt PI and PHI at rest and in transit.

33. **Logging and Monitoring**: Comstar shall implement and maintain an appropriate process to collect and audit logs and monitor network activity, such as through the use of a security information and event management ("SIEM") tool. Comstar shall further ensure that such tools are properly configured, regularly updated, and maintained to ensure that Security Incidents are analyzed in real-time, and that appropriate and timely follow-up is taken. In particular, Comstar shall create a formalized procedure to track alerts and Security Events as well as Comstar's response. Comstar shall further ensure that logs are secured and protected from alteration or destruction.

34. **Risk Assessments**: Comstar shall conduct annual risk assessments which must at a minimum include: (i) the identification of internal and external risks to the security, confidentiality, or integrity of PI and PHI; (ii) an assessment of the safeguards in place to control

these risks; (iii) the evaluation and adjustment of the Information Security Program considering the results of the assessment, including the implementation of reasonable safeguards to control these risks; and (iv) documentation of safeguards implemented in response to such annual risk assessments.

35. **Penetration Testing**: Comstar shall implement and maintain a penetration testing program reasonably designed to identify, assess, and remediate security vulnerabilities within its network. Such testing shall occur on at least an annual basis. Further, Comstar shall review the results of these tests, take reasonable steps to remediate any critical findings revealed by such testing, and document its decision-making regarding such remediation.

36. **Email Filtering and Phishing Solutions**: Comstar shall implement and maintain email protection and filtering solutions, including protection against email SPAM and phishing attacks, for its e-mail tenant user accounts.

37. **Antivirus Maintenance**: Comstar shall implement and maintain current, up-to-date antivirus protection programs or software on its network, which shall be at the highest technical level available.

38. **Data Loss Protection**: Comstar shall implement and maintain data loss prevention technology to detect and prevent unintentional disclosure or unauthorized exfiltration of PI or PHI.

39. **Intrusion Detection and Endpoint Detection**: Comstar shall implement and maintain an intrusion detection solution and controls designed to provide real-time notification of unauthorized access to its network, anomalous activity, and malicious system modifications within their network.

Information Security Program Assessment

40. Within one hundred and twenty (120) days of the Effective Date, Comstar shall obtain an information security assessment from an independent third-party assessor (Third-Party Assessor), that has not previously examined Comstar's systems, regarding its Information Security Program.

41. The Third-Party Assessment shall be conducted by a qualified, objective, independent third-party professional, who: (1) uses procedures and standards generally accepted in the profession; and (2) conducts an independent review of the Information Security Program.

42. The Third-Party Assessor shall prepare a report of its findings ("Report") which shall: (i) identify the specific administrative, technical, and physical safeguards maintained by Comstar; (ii) document the extent to which the identified safeguards are appropriate considering Comstar's size and complexity, the nature and scope of Comstar's activities, and the PI and PHI maintained by Comstar; (iii) assess the extent to which the identified safeguards meet the requirements of the Information Security Program;

43. Comstar shall provide a copy of the Report to the Attorney General no later than thirty (30) days after its completion.

III. PAYMENT TO THE STATES

44. Within thirty (30) days of the Effective Date, Comstar shall pay $415,000 to the Attorney General by wire transfer or by certified or cashier's check made payable to the "Commonwealth of Massachusetts" and delivered to Kaitlyn Karpenko, Assistant Attorney General, Privacy and Responsible Technology Division, One Ashburton Place, 18th Floor, Boston, MA 02108.

45. At her sole discretion, the Attorney General may distribute the payment described in this paragraph in any amount, allocation or apportionment and for any purpose permitted by

law, including but not limited to: (a) use by the Attorney General in the facilitation of this Final Judgment; (b) payments to the General Fund of the Commonwealth of Massachusetts; (c) payments to the Local Consumer Aid Fund established pursuant to G.L. c. 12, § 11G, and/or (d) for programs or initiatives in furtherance of the protection of the people of the Commonwealth.

IV. NOTICE/ DELIVERY OF DOCUMENTS

46. Whenever Comstar shall provide notice to the Attorney General under this Judgment, that requirement shall be satisfied by sending notice to

Laura Martella, *Assistant Attorney General*
Michele Lucan, *Deputy Associate Attorney General*
Office of the Attorney General
165 Capitol Avenue
Hartford, Connecticut 06106
(860) 808-5440
laura.martella@ct.gov
michele.lucan@ct.gov

Kaitlyn Karpenko, *Assistant Attorney General*
Office of the Attorney General
One Ashburton Place, 18th Floor
Boston, MA 02108
(617) 963-2341
kaitlyn.karpenko@mass.gov

V. GENERAL PROVISIONS

47. Comstar waives the requirement of G.L. c. 93H, § 6 and G.L. c. 93A, § 4 requiring five days written notice to the defendant prior to the Commonwealth commencing an action under G. L. c. 93A with respect to this matter and this Final Judgment.

48. Comstar waives all rights of appeal with respect to this Final Judgment.

49. Comstar waives all requirements of Rule 52 of the Massachusetts Rules of Civil Procedure with respect to the entry of this Final Judgment.

50. No part of this Final Judgment shall be construed to relieve Comstar of its obligations to comply with all applicable federal, state, and local laws, regulations, and rules.

51. Consent to this Final Judgment does not constitute an approval by the Commonwealth of any of Comstar' business acts or practices.

52. Any intentional violation of this Final Judgment, which is not cured within ninety (90) days written notice of the violation from the Attorney General, may be punishable by civil contempt proceedings, or as otherwise provided by law.

53. This Final Judgment becomes effective upon entry by the Court.

APPROVED AND ORDERED:

____
Justice of the Superior Court

DATED: ______________

CONSENT TO JUDGMENT BY COMSTAR, LLC

1. The Defendant, Comstar, LLC ("Comstar"), consents to the continuing subject matter jurisdiction, specific personal jurisdiction over Comstar, and venue of the Suffolk Superior Court, and hereby consents to the entry of the Final Judgment in the form attached hereto. In so consenting, Comstar certifies that they have read and understand each of the sections, paragraphs, and subparagraphs in the Final Judgment.

2. The parties waive the entry of findings of fact and conclusions of law under Rule 52 of the Massachusetts Rules of Civil Procedure.

3. Comstar understands that the obligations set forth in the Final Judgment apply to Comstar and its predecessors, successors, and assigns and shall constitute a continuing obligation.

4. Comstar states that it is represented by legal counsel, Freeman Mathis & Gary, LLP, and that Comstar's representative, Justin Boron, has personally read and understands each numbered paragraph in the Final Judgment by Consent.

5. The undersigned, Nicole Vessal represents that she is duly authorized to execute this Consent to Judgment on behalf of Comstar and to bind Comstar to all of its provisions, and that on behalf of Comstar he voluntarily enters into this Final Judgment by Consent.

6. Except for purposes of its enforcement, this Consent to Judgment shall not constitute evidence against Comstar.

ASSENTED TO, WAIVING ALL RIGHTS OF APPEAL

BY: ______________________________ Dated: 12-19-25

BBO Number: 703679