STATE OF CONNECTICUT

DOCKET NO. HHD-CV-26-6218477S	:	SUPERIOR COURT
STATE OF CONNECTICUT, *Plaintiff,*	:	JUDICIAL DISTRICT OF HARTFORD
v.	:	AT HARTFORD
COMSTAR, LLC *Defendant*.	:	JANUARY 28, 2026

FINAL JUDGMENT ON STIPULATION

Plaintiff, the State of Connecticut (the "State or the "Plaintiff"), appearing through William Tong, Attorney General of the State of Connecticut, and Defendant, Comstar, LLC have agreed to the stipulations and terms of this Final Judgment on Stipulation ("Judgment") without admission of any facts or liability of any kind as alleged in Plaintiff's Complaint, and with all parties having waived their right to appeal, and the Court having considered the matter and good cause appearing: IT IS HEREBY ORDERED, ADJUDGED, AND DECREED THAT:

I. PARTIES

1. Plaintiff is the State of Connecticut represented by William Tong, Connecticut Attorney General. The Attorney General, acting at the request of the Connecticut Commissioner of Consumer Protection, is charged with enforcement of Connecticut's Unfair Trade Practices Act ("CUTPA"), General Statutes § 42-110b *et seq*., the Data Breach Notification Law, General Statutes § 36a-701b, and the Safeguards Law, General Statutes § 42-471. The Attorney General is also authorized to enforce the Health Insurance Portability and Accountability Act 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) ("HIPAA").

2. 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.

3. As used herein, any reference to "Comstar" or "Defendant" shall mean Comstar, LLC including all its officers, directors, affiliates, subsidiaries, divisions, predecessors, successors, and assigns doing business in the United States.

II. BACKGROUND

4. The Attorneys General of Connecticut and Massachusetts (collectively, the "Attorneys General," or the "States") conducted an investigation of the ransomware attack that affected the Comstar computer network. Comstar discovered suspicious activity on its network on March 26, 2022, confirmed unauthorized access on April 21, 2022, and disclosed the incident to the States on May 25, 2022 ("Data Breach"), which impacted approximately 22,829 Connecticut residents and 326,426 Massachusetts residents. The Data Breach potentially compromised the highly sensitive personal and health information of those individuals, including their names, dates of birth, medical assessment and medication administration information, health insurance information, Social Security numbers and/or Medicare numbers.

5. The States' investigation examined the facts and circumstances of the Data Breach to determine whether Comstar complied with state consumer protection and privacy laws as well as HIPAA.

6. Defendant is entering into a Judgment with the States of Massachusetts and Connecticut and each State's 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.

III. STIPULATIONS

7. Plaintiff and Defendant agree to and do not contest the entry of this Judgment.

8. At all times relevant to this matter, Defendant Comstar engaged in trade and commerce affecting Connecticut consumers, in that Comstar is an ambulance billing and collection company that maintained Connecticut residents' sensitive personal and health information in connection with its services.

9. Defendant Comstar is subject to the requirements of the Consumer Protection Act, Personal Information Protection Act, and Data Breach Notification Law, as defined below. Comstar is also a Business Associate subject to the requirements of HIPAA.

10. Defendant Comstar consents to jurisdiction and venue for purposes of entry of this Judgment as well as for the purpose of any subsequent action to enforce it.

IV. JURISDICTION

11. The Court finds it has jurisdiction over Comstar for purposes of entry of this Judgment as well as for the purpose of any subsequent action to enforce it.

12. The Court finds that it has jurisdiction over the subject matter and over the Parties for the purpose of entering and enforcing this Judgment, and venue is proper in this Court pursuant to CUTPA. This Judgment is entered pursuant to CUTPA, and more specifically General Statutes § 42-110m. 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 Judgment.

V. DEFINITIONS

13. "Consumer Protection Act" shall mean Connecticut's Unfair Trade Practices Act ("CUTPA"), General Statutes § 42-110b *et seq*.

14. "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.

15. "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**.**

16. "Data Breach Notification Law" shall mean Connecticut's Data Breach Notification Law, General Statutes § 36a-701b.

17. "Effective Date" shall be February 28, 2026.

18. "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.

19. "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.

20. "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.

21. "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).

22. "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.

23. "Personal Information" or "PI" shall have the same meaning as set forth in General Statutes §§ 36a-701b(a)(2) and 42-471(c).

24. "Protected Health Information" or "PHI" is defined in accordance with 45 C.F.R. § 160.103.

25. "Personal Information Protection Act" shall mean Connecticut's Safeguards Law, General Statutes § 42-471.

26. "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.

VI. INJUNCTIVE RELIEF

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

Compliance with State and Federal Laws

28. 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.

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

30. 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

31. 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"). The Information Security Program shall, at a minimum, include the specific information security safeguards set forth in Paragraphs 40 through 51 of this Judgment.

32. 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.

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

34. 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.

35. 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.

36. 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.

37. 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.

38. 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.

39. 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

40. **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 only retain records related to patient transportation that were created more than two years from the date of service to the patient if the record is legally required to be retained for more than two years and if the record is maintained in a local hard disk that is not accessible by network or virtual access ("Archiving"). At a minimum, Archiving shall be performed on a quarterly basis.

41. **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 to those at Comstar who need such information to perform their job duties.

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).

42. **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.

43. **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.

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

45. **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.

46. **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.

47. **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.

48. **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.

49. **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.

50. **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.

51. **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

52. 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) regarding its Information Security Program.

53. 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.

54. 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;

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

VII. PAYMENT TO THE STATES

56. Within thirty (30) days of the Effective Date, Comstar shall pay $100,000.00 to the Attorney General payable to the Treasurer, State of Connecticut which will be deposited in the General Fund. Said payment may be used by the Attorney General for purposes that may include, but are not limited to, attorney's fees and other costs of investigation and litigation, or be placed in, or applied to, any consumer protection law enforcement fund, including consumer protection or privacy enforcement, consumer education, litigation or local consumer aid fund, or for such other uses permitted by state law, at the sole discretion of the state's Attorney General. If the Court has not entered this Judgment by its Effective Date, Comstar shall make the payment within fourteen (14) days of the entry of Judgment.

57. Following full payment of the amounts due by Comstar under this Judgment, the Attorney General shall release and discharge Comstar from civil claims that the Attorney General could have brought arising from the Data Breach under the Consumer Protection Act, Personal Information Act, Data Breach Notification Law and HIPAA. Nothing contained in this paragraph shall be construed to limit the ability of the Attorney General to enforce the obligations that Defendant, or its officers, subsidiaries, affiliates, agents, representatives, employees, successors, and assigns have under this Judgment.

VIII. NOTICE/ DELIVERY OF DOCUMENTS

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

Laura J. 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

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

Nicole E. Vessal, Vice President
Comstar
Ambulance Billing Service
8 Turcotte Memorial Drive
Rowley, MA 01969
(978) 356-3344
nvessal@comstarbilling.com

IX. GENERAL PROVISIONS

60. The terms of this Judgment are not intended to be construed as an admission or concession or evidence of liability or wrongdoing on the part of Defendant.

61. Acceptance and entry of this Judgment is not an approval of any of Defendant's business practices.

62. Defendant will not participate in any activity to form a separate entity for the purpose of engaging in acts or practices prohibited by this Judgment or for any other purpose that would circumvent this Judgment.

63. Nothing in this Judgment shall be construed to limit the authority of the State to protect the interests of the State or its citizens, or to enforce any laws, regulations, or rules against Defendant.

64. This Judgment does not affect any private right of action that any consumer, person, entity, or federal, state, or local governmental entity may have against Defendant.

65. Nothing in this Judgment waives or affects any claims of sovereign immunity by the State.

66. Defendant expressly waives any rights, remedies, appeals, or other interests related to a jury trial or any related or derivative rights under the Connecticut or United States Constitutions or other laws as to this Judgment.

67. This Court must approve all modifications to this Judgment.

68. If any provision of this Judgment shall be held unenforceable, the Judgment shall be construed as if such provision did not exist.

69. This Judgment may be executed in counterparts that, together, will constitute one whole document.

70. Within 30 days of this Judgment's entry, Defendant shall provide a copy of this Judgment to each of their officers and directors, and owners. Once provided, Defendant shall, within 45 days of this Judgment's entry, provide a certification under oath to the State that affirms compliance with this paragraph.

71. All costs associated with this action and Judgment shall be borne by Defendant's Payment to the States, and no costs shall be taxed to the States.

72. This Judgment sets forth the entire agreement between the parties.

JOINTLY APPROVED AND SUBMITTED FOR ENTRY:

PLAINTIFF, THE STATE OF CONNECTICUT

WILLIAM TONG,
Attorney General

By: Laura J. Martella Date: 1/28/26

Laura J. 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

DEFENDANT, COMSTAR, LLC

By: _____ Date: 1-27-26

Nicole E. Vessal
Vice President
Comstar
Ambulance Billing Service
8 Turcotte Memorial Drive
Rowley, MA 01969

COUNSEL FOR DEFENDANT COMSTAR

By: _____ Date: 1/27/2026

Tara A. Sheldon, Esq.
Local Counsel for Comstar, LLC
Freeman Mathis & Gary, LLP
185 Asylum Street, 6th Floor
Hartford, CT 06103
Firm Juris No. 440729
Phone: 959-202-5256
Email: Tara.Sheldon@fmglaw.com

and

Justin J. Boron
Lead Counsel for Comstar, LLC
Freeman Mathis & Gary, LLP
1600 Market Street, Suite 2700
Philadelphia, PA 19103-7401
Phone: (215) 789-4919
Email: Justin.Boron@fmglaw.com