NEW YORK STATE
DEPARTMENT OF FINANCIAL SERVICES
ONE STATE STREET
NEW YORK, NEW YORK 10004

----------x

In the Matter of :

TTEC HEALTHCARE SOLUTIONS, INC. :

----------x

**CONSENT ORDER**

The New York State Department of Financial Services (the "Department" or "DFS") and TTEC Healthcare Solutions, Inc., ("TTEC HS" or the "Company") (together, the "Parties") agree to resolve the matters described herein without further proceedings.

WHEREAS, TTEC HS is licensed by the Department to sell life and health insurance in New York State;

WHEREAS, August 29, 2017 marked the initial effective date of New York's first-in the-nation cybersecurity regulation, 23 NYCRR Part 500 (the "Cybersecurity Regulation");

WHEREAS, the Cybersecurity Regulation defines clear standards for cooperative industry compliance, robust consumer data protection, vital cybersecurity controls, timely reporting of Cybersecurity Events, as defined by 23 NYCRR § 500.01(d), and was promulgated to strengthen cybersecurity and data protection for the industry and consumers;

WHEREAS, the Department has been investigating a Cybersecurity Event that was experienced within TTEC HS as well as TTEC HS's compliance with the Cybersecurity Regulation;

WHEREAS, based on the investigation, the Department has concluded that TTEC HS violated the following sections of the Cybersecurity Regulation: (1) TTEC HS did not have multi-factor authentication fully implemented for all users in the United States and did not have reasonably equivalent or more secure access controls approved in writing by the Company's Chief Information Security Officer(s) ("CISO"), in violation of 23 NYCRR § 500.12(b); (2) TTEC HS failed to maintain, for the required three years, audit trails designed to detect and respond to Cybersecurity Events, in violation of 23 NYCRR § 500.06(b); (3) TTEC HS improperly certified compliance with the Cybersecurity Regulation for the 2020 calendar year, in violation of 23 NYCRR § 500.17(b); and (4) TTEC HS did not file a certification of compliance with the Cybersecurity Regulation for the calendar years 2018 and 2019, in violation of 23 NYCRR § 500.17(b); and;

NOW THEREFORE, to resolve this matter without further proceedings pursuant to the Superintendent's authority under Section 408 of the New York Financial Services Law, the Department finds as follows:

## THE DEPARTMENT'S FINDINGS

Introduction

1. The Department is the insurance regulator of the State of New York, and the Superintendent of Financial Services is responsible for ensuring the safety and soundness of New York's insurance industry and promoting the reduction and elimination of fraud, abuse, and unethical conduct with respect to insurance licensees.

2. The Superintendent has the authority to conduct investigations, bring enforcement proceedings, levy monetary penalties, and order injunctive relief against parties who have violated the relevant laws and regulations.

3. Among the Superintendent's many roles is a consumer protection function, which includes the protection of individuals' private and personally sensitive data from careless, negligent, or willful exposure by licensees of the Department.

4. To support this critical role, the Cybersecurity Regulation places on all DFS-regulated entities ("Covered Entities") an obligation to establish and maintain a cybersecurity program designed to protect the confidentiality, integrity, and availability of its Information Systems, as well as any non-public information ("NPI") belonging to consumers contained therein. 23 NYCRR §§ 500.01(c), 500.01(e), 500.01(g), 500.02(a).

5. In addition to 23 NYCRR § 500.17(b), which requires Covered Entities to certify compliance with the Cybersecurity Regulation on an annual basis, the Cybersecurity Regulation also contains requirements to protect licensed entities' internal networks from threat actors seeking to access and exploit NPI.

6. Section 500.12(b) of the Cybersecurity Regulation requires that Covered Entities implement multifactor authentication ("MFA") "for any individual accessing the Covered Entity's internal networks from an external network, unless the Covered Entity's CISO has approved in writing the use of reasonably equivalent or more secure access controls." 23 NYCRR §500.12(b). MFA requires two or more distinct authentication factors for successful access, such that username and password credentials alone are insufficient for access. 23 NYCRR §§ 500.01(f). MFA is an important line of defense against attempts to gain unauthorized access to accounts, including through phishing emails — *i.e.*, emails sent by cyber attackers to

deceive users into providing their credentials, or personal or other confidential information to permit unauthorized access or harm to protected information systems.

7. Section 500.06(a)(2) of the Cybersecurity Regulation requires that Covered Entities shall securely maintain systems that "include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity." These records must be maintained for not fewer than three years. 23 NYCRR § 500.06(b).

Events at Issue

*Ransomware Cyber Event*

8. TTEC HS reported a Cybersecurity Event to the Department on October 4, 2021 (the "Ransomware Cyber Event"). TTEC HS discovered the Ransomware Cyber Event on September 12, 2021, when it determined that certain devices on its network had been encrypted with ransomware. Employees of TTEC HS notified the Company's IT department that certain Information Systems were infiltrated and could not be accessed. Approximately 1,800 devices were compromised by the ransomware.

9. Prior to executing the ransomware attack on September 12, 2021, threat actors exfiltrated data from the TTEC HS network, including NPI of current and former employees of TTEC HS, and for insureds and former insureds of one TTEC HS's client, including New York residents.

10. Once the ransomware was discovered, TTEC HS activated its incident response and business continuity protocols, isolated the systems involved, and took other measures to contain the incident and to restore operations within several hours of being notified of the attack.

11. TTEC HS's investigation into the Ransomware Cyber Event concluded that threat actors likely gained access to the Company's network in late March 2021 through a phishing email sent to a network administrator. At that time, TTEC HS did not have adequate MFA controls in place. As a result, the threat actors exported the administrator's security certificate from the administrator's computer to another machine and moved unencumbered throughout the TTEC HS network until being discovered on September 12, 2021.

12. TTEC HS did not begin to broadly implement MFA until after the COVID-19 pandemic required its entire workforce to work from home beginning in March 2020. At that time and throughout the time the threat actors had access to the TTEC HS systems, TTEC HS users utilized Secure SSL certificates ("Security Certificates") in order to access TTEC HS's IT environment. These security certificates were used in addition to users' passwords to authenticate users as TTEC HS began deployment of MFA systems throughout its entire workforce. However, the security certificates did not meet the standard of "reasonably equivalent or more secure access controls", as required by the Cybersecurity Regulation, and furthermore, were not approved in writing by TTEC HS's CISO.

13. MFA implementation Company-wide is ongoing.

14. At the time of the Ransomware Cyber Event, TTEC HS only maintained active audit trail records for ninety (90) days, with archived audit trail records maintained for an additional fifteen (15) months. However, the audit trail records were insufficient to effectively assist TTEC in detecting and responding when the threat actors gained access to its Information Systems. In any event, TTEC did not maintain its audit trail records for the three (3) years required by the Cybersecurity Regulation.

*Part 500 Compliance Certification*

15. Pursuant to 23 NYCRR § 500.17(b), Covered Entities are required annually to certify their compliance with the Cybersecurity Regulation.

16. Without any discussion or notification to the Department as to why, TTEC HS did not file a certification of compliance with the Cybersecurity Regulation for the 2018 or 2019 calendar years, in violation of Section 500.17(b).

17. Thereafter, while TTEC HS timely certified compliance for the 2020 calendar year, on April 15, 2021, at that time TTEC HS did not have MFA in place for all of its users and did not maintain audit trails for the required period of time, and therefore was not in compliance with the Cybersecurity Regulation at the time of certification and the certification for the 2020 calendar year was improper, in violation of Section 500.17(b).

Violations of Law and Regulations

18. At the time of the Ransomware Cyber Event, TTEC HS had not fully implemented MFA for all users and the Company's CISO had not approved in writing any reasonably equivalent or more secure access controls, in violation of 23 NYCRR § 500.12(b).

19. TTECH HS does not maintain audit trail records for at least three years, in violation of 23 NYCRR § 500.06(b).

20. The Company improperly certified compliance with the Cybersecurity Regulation for the 2020 calendar year, in violation of 23 NYCRR § 500.17(b).

21. The Company did not file a certification of compliance with the Cybersecurity Regulation for the calendar years 2018 and 2019, in violation of 23 NYCRR § 500.17(b).

NOW THEREFORE, to resolve this matter expeditiously and without further proceedings, the Department and the Company stipulate and agree to the following terms and conditions:

## SETTLEMENT PROVISIONS

Monetary Penalty

22. No later than ten (10) days after the Effective Date (as defined below) of this Consent Order, TTEC HS shall pay a total civil monetary penalty pursuant to Financial Services Law § 408 to the Department in the amount of One Million Nine Hundred Thousand U.S. Dollars ($1,900,000.00). The payment shall be in the form of a wire transfer in accordance with instructions provided by the Department.

23. TTEC HS shall not claim, assert, or apply for a tax deduction or tax credit with regard to any U.S. federal, state, or local tax, directly or indirectly, for any portion of the civil monetary penalty paid pursuant to this Consent Order.

24. TTEC HS shall neither seek nor accept, directly or indirectly, reimbursement or indemnification with respect to payment of the penalty amount, including but not limited to, payment made pursuant to any insurance policy.

25. In assessing a penalty for failures in cybersecurity compliance and required reporting, the Department has taken into account factors that include, without limitation: the extent to which TTEC HS has cooperated with the Department in the investigation of such conduct, its prompt response to the incident, the gravity of the violations, and such other matters as justice and the public interest may require.

26. The Department acknowledges TTEC HS's commendable cooperation throughout the investigation of the Ransomware Cyber Event. The Department also recognizes TTEC HS's

disclosure to the Department of the cybersecurity issues known to TTEC HS at the time of the Ransomware Cyber Event and ongoing efforts to remediate the shortcomings identified in this Consent Order. Among other things, TTEC HS has demonstrated its commitment to remediation by devoting significant financial and other resources to enhance its cybersecurity program, including through changes now underway to its policies, procedures, systems, governance structures, training, and personnel.

Remediation

27. TTEC HS shall continue to strengthen its controls to protect its cybersecurity systems and consumers' NPI in accordance with the requirements of the Cybersecurity Regulation.

28. Cyber Maturity Assessment.

a. Within one hundred and twenty (120) days of the Effective Date of this Consent Order, the Company shall complete a Cyber Maturity Assessment to review its cybersecurity infrastructure and environment following the remediation efforts it has undertaken since the Ransomware Cyber Event (the "CMA"). The Company shall notify the Department of the completion of the CMA.

b. Within ninety (90) days of the conclusion of the CMA, the Company shall submit to the Department a copy of the results of the CMA, together with a report prepared by the Company containing any steps the Company will take, or has already taken, to address recommendations contained in the CMA.

29. MFA Audit. Within one hundred twenty (120) days of the Effective Date of this Consent Order, the Company shall hire a third-party auditor to conduct an audit of current MFA controls in the various environments utilized by TTEC HS and submit the results of the same to

the Department. This MFA Audit shall be tailored to assess the Company's MFA access points and protection of NPI. Upon completion, a copy of the third-party audit will be provided to the Department. To the extent any material issues are discovered, the Company is to remediate those issues within a reasonable timeframe agreed to by the Department following the issuance of any report or findings by the third-party conducting the audit.

30. Audit Trail Implementation and Audit. Within one hundred twenty (120) days of the Effective Date of this Order, the Company shall hire a third-party auditor to conduct an audit of TTEC HS's audit trail record retention policy and develop a plan for becoming compliant with Part 500.06 requirements. Upon completion, a copy of the third-party audit will be provided to the Department.

31. Information Security Dashboard. Within one hundred twenty (180) days of the Effective Date of this Order, the Company will develop an information reporting system that tracks all Information Security functions taking place at the Company and that can be accessed by executives overseeing Information Security. Screenshots or samples of such system will be made available to the Department upon request.

Full and Complete Cooperation

32. TTEC HS commits and agrees that it will fully cooperate with the Department regarding all the terms of this Consent Order.

Further Action by the Department

33. No further action will be taken by the Department against the Company or its successors for the conduct set forth in this Consent Order as it relates to the Ransomware Cyber Event that occurred on September 12, 2021, and the Department's investigation related to the same (detailed herein), or in connection with the remediation set forth in this Consent Order,

provided that the Company fully complies with the terms of the Consent Order.

34. Notwithstanding any other provision of this Consent Order, however, the Department may undertake additional action against the Company for transactions or conduct that were not disclosed in the written materials submitted to the Department or conversations between the Company and the Department in connection with this matter.

35. The Department reserves the right to investigate any other part of the TTEC HS cybersecurity program not directly covered by this Consent Order and undertake additional action against the Company as the Department deems appropriate.

Waiver of Rights

36. The Company submits to the authority of the Superintendent to effectuate this Consent Order.

37. The parties understand and agree that no provision of this Consent Order is subject to review in any court, tribunal, or agency outside of the Department.

Parties Bound by the Consent Order

38. This Consent Order is binding on the Department and the Company, as well as any successors and assigns. This Consent Order does not bind any federal or other state agency or any law enforcement authority.

Breach of Consent Order

39. In the event that the Department believes TTEC HS to be in material breach of the Consent Order, the Department will provide written notice to the Company, and the Company must, within ten (10) days of receiving such notice, or on a later date if so determined in the Department's sole discretion, appear before the Department to demonstrate that no

material breach has occurred or, to the extent pertinent, that the breach is not material or has been cured.

40. TTEC HS understands and agrees that its failure to make the required showing within the designated time period shall be presumptive evidence of the Company's breach. Upon a finding that a breach of this Consent Order has occurred, the Department has all the remedies available to it under the New York Insurance and Financial Services Laws, and any other applicable laws, and may use any evidence available to the Department in any ensuing hearings, notices, or orders.

Notices

41. All notices or communications regarding this Consent Order shall be sent to:

For the Department:

Madeline W. Murphy
Assistant Deputy Superintendent
Consumer Protection and Financial Enforcement Division
New York State Department of Financial Services
One Commerce Plaza
Albany, NY 12257

John A. Nicosia
Senior Assistant Deputy Superintendent
Consumer Protection and Financial Enforcement Division
New York State Department of Financial Services
One State Street
New York, NY 10004

For TTEC HS:

Shannon Brennan
Chief Regulatory Counsel
TTEC Holdings Inc.
9197 South Peoria Street
Englewood, CO 80112-5833

Margaret McLean
General Counsel
TTEC Holdings Inc.
9197 South Peoria Street
Englewood, CO 80112-5833

Cynthia J. Borrelli
Bressler, Amery, & Ross, P.C.
17 State Street
Floor 34
New York, NY 10004

Miscellaneous

42. This Consent Order and any dispute thereunder shall be governed by the laws of the State of New York without regard to any conflicts of laws principles.

43. This Consent Order may not be altered, modified, or changed unless in writing and signed by the parties hereto.

44. This Consent Order constitutes the entire agreement between the Department and the Company and supersedes any prior communication, understanding, or agreement, whether written or oral, concerning the subject matter of this Consent Order.

45. Each provision of this Consent Order shall remain effective and enforceable against the Company, its successors, and assigns, until stayed, modified, suspended, or terminated by the Department.

46. In the event that one or more provisions contained in this Consent Order shall for any reason be held to be invalid, illegal, or unenforceable in any respect, such invalidity, illegality, or unenforceability shall not affect any other provision of this Consent Order.

47. No promise, assurance, representation, or understanding other than those contained in this Consent Order has been made to induce any party to agree to the provisions of this Consent Order.

48. Nothing in this Consent Order shall be construed to prevent any consumer from pursuing any right or remedy at law.

49. This Consent Order may be executed in one or more counterparts and shall become effective when such counterparts have been signed by each of the parties hereto (the "Effective Date").

*[remainder of this page intentionally left blank]*

IN WITNESS WHEREOF, the parties have caused this Consent Order to be signed on the dates set forth below.

**NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES**

By: /s/ Madeline W. Murphy
MADELINE W. MURPHY
Assistant Deputy Superintendent for Consumer Protection and Financial Enforcement

November 29, 2022

By: /s/ Terri-Anne S. Caplan
TERRI-ANNE S. CAPLAN
Deputy Director of Enforcement for Consumer Protection and Financial Enforcement

November 29, 2022

By: /s/ Kevin R. Puvalowski
KEVIN R. PUVALOWSKI
Acting Executive Deputy Superintendent for Consumer Protection and Financial Enforcement

December 2, 2022

**TTEC HEALTHCARE SOLUTIONS INC.**

By: /s/ Dustin Semach
DUSTIN SEMACH
Chief Financial Officer

November 28, 2022

**THE FOREGOING IS HEREBY APPROVED. IT IS SO ORDERED.**

/s/ Adrienne A. Harris
ADRIENNE A. HARRIS
Superintendent of Financial Services

December 2, 2022