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

----------x

In the Matter of :

DELTA DENTAL INSURANCE COMPANY, and :
DELTA DENTAL OF NEW YORK, INC.
:

----------x

CONSENT ORDER

The New York State Department of Financial Services (the "Department" or "DFS") and Delta Dental Insurance Company ("DDIC") and Delta Dental of New York, Inc. ("DDNY") (together, the "Companies") are willing to resolve the matters described herein without further proceedings.

WHEREAS, DDIC is licensed by the Department as an accident and health insurer, and DDNY is licensed by the Department as a non-profit dental expense indemnity;

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");[1]

[1] Citations and other references to 23 NYCRR Part 500 herein refer to the Cybersecurity Regulation as it read prior to November 1, 2023.

WHEREAS, the Cybersecurity Regulation defines clear standards and guidelines for cooperative industry compliance, robust consumer data protection, vital cybersecurity controls, and timely reporting of Cybersecurity Events, as defined by 23 NYCRR § 500.1(d), and was promulgated to strengthen cybersecurity and data protection for the industry and consumers;

WHEREAS, the Companies are Covered Entities within the meaning of 23 NYCRR § 500.1(c) and are required to comply with the Cybersecurity Regulation;

WHEREAS, the Companies are affiliates in the Insurance Holding Company System of Delta Dental of California and use the cybersecurity program of Delta Dental of California ("DDC"), as permitted by 23 NYCRR § 500.2(c);

WHEREAS, the Department initiated an investigation into a Cybersecurity Event experienced by DDC and the Companies in May 2023 and reported by the Companies to the Department on December 15, 2023; and

WHEREAS, based on its investigation, the Department has concluded that the Companies violated the following sections of the Cybersecurity Regulation: (1) 23 NYCRR § 500.13, which requires Covered Entities to have policies and procedures for the secure disposal, on a periodic basis, of any Nonpublic Information ("NPI") that is no longer necessary for business operations or for other legitimate business purposes; (2) 23 NYCRR § 500.3(n), which requires Covered Entities to implement and maintain a written policy that addresses incident response, which includes providing sufficient detail and guidance concerning the Covered Entity's regulatory reporting obligations to the Department; (3) 23 NYCRR § 500.16(b)(6), which requires Covered Entities to establish a written incident response plan that addresses, *inter alia*, reporting of Cybersecurity Events; and (4) 23 NYCRR § 500.17(a), which requires Covered Entities to provide timely notice of Cybersecurity Events to the Department.

NOW THEREFORE, to resolve this matter without further proceedings, 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 has the authority to conduct investigations, bring enforcement proceedings, levy monetary penalties, and order injunctive relief against licensees that have violated the relevant laws and regulations.

2. Among the Superintendent's roles is a consumer protection function, which includes the critical protection of individuals' private and personally sensitive data from exposure by licensees of the Department.

3. To support this important role, the Superintendent's Cybersecurity Regulation places on all Covered Entities, including the Companies, the obligation to establish and maintain a cybersecurity program designed to protect the confidentiality and integrity of their Information Systems, as well as any NPI contained thereon. 23 NYCRR §§ 500.1(c), 500.1(e), 500.1(g), 500.2(a), 500.3.

4. To ensure the security and protection of NPI and prevent Cybersecurity Events, Covered Entities must implement policies and procedures for the secure disposal, on a periodic basis, of any NPI that is no longer necessary for business operations or for other legitimate business purposes of the Covered Entities. 23 NYCRR § 500.13.

5. Moreover, Covered Entities must implement and maintain policies addressing incident response and must establish an incident response plan that addresses how Covered

Entities will comply with their obligations to report Cybersecurity Events to regulators. 23 NYCRR §§ 500.3(n), 500.16(b)(6).

6. Specifically, the Cybersecurity Regulation requires Covered Entities to notify the Department of a Cybersecurity Event promptly and in no event later than 72 hours after a determination that an event has occurred that requires notice to any government body, self-regulatory agency, or any other supervisory body, or has a reasonable likelihood of materially harming any material part of normal operations. This obligation of Covered Entities is paramount, as the failure to provide the Department with prompt notice of a Cybersecurity Event hinders the Department's ability to provide timely and relevant guidance to the industry to prevent or mitigate similar Cybersecurity Events. 23 NYCRR § 500.17(a).

Events at Issue

The Cybersecurity Event

7. DDC licenses the use of MOVEit Transfer from Progress Software Corporation ("Progress") to facilitate the transfer of files on behalf of DDC and its affiliates, including the Companies, to and from other affiliates, customers, business partners, providers, and employees. Some of the files transferred via MOVEit Transfer, including eligibility- and claims-related files, contain NPI of insureds.

8. On June 1, 2023, Progress released a security advisory concerning a previously unknown zero-day vulnerability that enabled threat actors to gain unauthorized access to MOVEit Transfer.

9. Also on June 1, 2023, DDC received an alert from its CrowdStrike endpoint detection and response tool regarding potentially suspicious activities related to MOVEit Transfer. That same day, DDC identified the presence of a webshell on the MOVEit Transfer

servers related to the vulnerability identified by Progress. Upon this discovery, DDC stopped access to MOVEit Transfer, removed the malicious files, conducted an analysis of the MOVEit Transfer database, deployed all patches and security updates provided by Progress to remediate the vulnerability, and reset administrative passwords to MOVEit Transfer.

10. Contemporaneously, DDC initiated an internal investigation to determine whether threat actors had exploited the zero-day vulnerability and gained unauthorized access to files on MOVEit Transfer.

11. On July 6, 2023, DDC discovered evidence that, between May 28 and May 30, 2023, threat actors had exploited the vulnerability and exfiltrated files from MOVEit Transfer.

12. Based on a forensic review that concluded on November 27, 2023, DDC determined that threat actors had exfiltrated approximately 60,000 files. The exfiltrated files contained a variety of data, including insureds' names, addresses, social security numbers, driver's license and other state identification numbers, passport numbers, financial account information, tax identification numbers, health insurance policy numbers, and patient health information.

The Companies' Failure to Have Policies and Procedures for the Secure and Periodic Disposal of NPI

13. Section 500.13 of the Cybersecurity Regulation requires Covered Entities to implement and maintain "policies and procedures for the secure disposal on a periodic basis of any Nonpublic Information . . . that is no longer necessary for business operations or for other legitimate business purposes of the Covered Entit[ies]." 23 NYCRR § 500.13.

14. MOVEit Transfer permits DDC to create folders for specific customers, providers, or projects to enable the transfer of files as described in paragraph 7.

15. Additionally, MOVEit Transfer preconfigures each folder with a default retention setting of 30 days, after which a file uploaded to a folder is deleted from MOVEit Transfer. DDC had the ability to shorten, extend, or disable MOVEit Transfer's default retention settings on a folder-by-folder or file-by-file basis. At the time of the Cybersecurity Event, DDC had extended the retention setting to 45 or 60 days for many folders and, in some instances, disabled folders' retention settings entirely.

16. DDC, however, had no written policy or procedure for requesting, reviewing, or approving such changes to folder retention settings.

17. As a result of DDC's changes to the default retention settings, the majority of the exfiltrated files on MOVEit Transfer at the time of the Cybersecurity Event were in folders that had retention settings that were longer than 30 days, and the majority of the exfiltrated files had been on the servers longer than 30 days.

The Companies' Incident Response Policy and Reporting Failures

18. The Cybersecurity Regulation requires Covered Entities to implement and maintain a written policy addressing incident response, which encompasses regulatory reporting obligations, and establish a written response plan designed to address, *inter alia*, their regulatory reporting obligations. 23 NYCRR §§ 500.3(n), 500.16(b)(6).

19. Section 500.17 of the Cybersecurity Regulation requires Covered Entities to notify the Superintendent within 72 hours of determining that a Cybersecurity Event has occurred that either requires notice to be given to any "government body, self-regulatory agency or any other supervisory body" or has a "reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity." 23 NYCRR § 500.17(a).

20. Further, on June 2, 2023, the Department published to its website an industry letter alerting Covered Entities to the MOVEit Transfer vulnerability. This guidance specifically reminded entities of their obligations to report Cybersecurity Events and stated that "DFS considers evidence of unauthorized access to information systems, such as webshell installation, even if there has been no malware deployed or data exfiltrated, a reportable Cybersecurity Event…."[2]

21. Despite having identified the presence of a webshell on June 1, 2023, and having determined by July 6, 2023, that data had been exfiltrated from the MOVEit Transfer servers, the Companies did not notify the Department of the Cybersecurity Event until December 15, 2023.

22. In delaying notice to December 15, 2023, the Companies failed to comply with their obligation to provide timely notice to the Superintendent under § 500.17(a).

23. DDC's incident response policies and procedures lacked sufficient detail and guidance concerning the Companies' regulatory reporting obligations, including their reporting obligations to the Department, which contributed to the Companies' failure to timely report the Cybersecurity Event to the Superintendent.

Violations of Law and Regulations

24. The Companies failed to implement and maintain a written policy addressing incident response, in violation of 23 NYCRR § 500.3(n).

25. The Companies' cybersecurity program failed to include policies and procedures for the secure disposal, on a periodic basis, of NPI that is no longer necessary for business

[2] https://www.dfs.ny.gov/industry_guidance/industry_letters/il20230602_moveit_vulnerability.

operations or for other legitimate business purposes of the Companies, in violation of 23 NYCRR § 500.13.

26. The Companies failed to establish a written incident response plan that sufficiently addressed their reporting obligations to regulators, in violation of 23 NYCRR § 500.16(b)(6).

27. The Companies failed to provide timely notice of the Cybersecurity Event to the Department, in violation of 23 NYCRR § 500.17(a).

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

SETTLEMENT PROVISIONS

Monetary Penalty

28. No later than ten (10) days after the Effective Date (as defined below) of this Consent Order, the Companies shall pay a total civil monetary penalty to the Department in the amount of Two Million, Two Hundred Fifty Thousand U.S. Dollars and 00/100 Cents ($2,250,000.00). The payment shall be in the form of a wire transfer in accordance with instructions provided by the Department.

29. The Companies 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.

30. The Companies 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.

31. In assessing a civil monetary penalty, the Department has taken into account factors that include, without limitation, the extent to which the Companies cooperated with the Department in the investigation of such conduct, the gravity of the violations, and such other matters as justice and the public interest may require.

32. The Department acknowledges the Companies' cooperation throughout this investigation, prompt investigation of the Cybersecurity Event, and continued remediation of the issues identified in this order.

Full and Complete Cooperation

33. The Companies commit and agree that they will fully cooperate with the Department regarding all terms of this Consent Order.

Further Action by the Department

34. No further action will be taken by the Department against the Companies or their successors for the conduct set forth in this Consent Order, provided that the Companies fully comply with the terms of the Consent Order.

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

Waiver of Rights

36. The Companies submit 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 Companies, 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 the Companies to be in material breach of the Consent Order, the Department will provide written notice to the Companies, and the Companies 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. The Companies understand and agree that their failure to make the required showing within the designated time period shall be presumptive evidence of the Companies' 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 Law and Financial Services Law, 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:

Christina Glekas
Enforcement Counsel
Consumer Protection and Financial Enforcement
New York State Department of Financial Services
One State Street
New York, NY 10004

For the Companies:

Kari M. Rollins
Outside Counsel
Sheppard Mullin Richter & Hampton LLP
30 Rockefeller Plaza
New York, New York 10112

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 Companies 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 Companies, their 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 or any other third party from pursuing any right or remedy at law.

49. Except with regard to the enforcement of this Consent Order, the Companies' consent to the provisions of this Consent Order is not intended to bar, estop, waive, preclude, or otherwise prevent the Companies from taking any position of law or fact or raising any defenses in any action taken by any federal or state agency or department, or in any civil action brought by any party against the Companies.

50. 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/ Christopher J. Hummel
CHRISTOPHER J. HUMMEL
Senior Enforcement Counsel Consumer Protection and Financial Enforcement

April 29, 2026

By: /s/ Alison L. Passer
ALISON L. PASSER
Deputy Superintendent
Consumer Protection and Financial Enforcement

April 29, 2026

By: /s/ R. Gabriel D. O'Malley
R. GABRIEL D. O'MALLEY
Executive Deputy Superintendent
Consumer Protection and Financial Enforcement

April 29, 2026

DELTA DENTAL INSURANCE COMPANY

By: /s/ Michael Hankinson
MICHAEL HANKINSON
President

April 27, 2026

DELTA DENTAL OF NEW YORK, INC.

By: /s/ Michael Hankinson
MICHAEL HANKINSON
Executive Vice President & Chief Legal Officer

April 27, 2026

THE FOREGOING IS HEREBY APPROVED. IT IS SO ORDERED.

/s/ Kaitlin Asrow
KAITLIN ASROW
Acting Superintendent of Financial Services

April 29, 2026