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

----------x

In the Matter of :

THE TRAVELERS INDEMNITY
COMPANY :

----------x

CONSENT ORDER

The New York State Department of Financial Services (the "Department" or "DFS") and The Travelers Indemnity Company ("Travelers" or the "Company") are willing to resolve the matters described herein without further proceedings.

WHEREAS, Travelers is licensed by the Department to sell property and casualty 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 § 500.1(d), and was promulgated to strengthen cybersecurity and data protection for the industry and consumers;

WHEREAS, Travelers shares a Cybersecurity Program with its parent, The Travelers Companies, Inc. ("The Travelers Companies"), as well as other subsidiaries of The Travelers Companies, as is permitted pursuant to 23 NYCRR § 500.2(c);

WHEREAS, the Department has been investigating a Cybersecurity Event experienced at Travelers, as well as the Company's general compliance with the Cybersecurity Regulation; and

WHEREAS, based on the investigation, the Department concluded that Travelers violated the following sections of the Cybersecurity Regulation: (1) 23 NYCRR § 500.3 (d), & (k), which require that Covered Entities implement and maintain written cybersecurity policies that address, *inter alia*, access controls and identity management, and customer data privacy; (2) 23 NYCRR § 500.7, which requires Covered Entities to limit user access privileges to Information Systems that provide access to Nonpublic Information ("NPI"); and (3) 23 NYCRR § 500.12(a), which requires that Covered Entities use effective controls to protect against unauthorized access to NPI or Information Systems.

NOW THEREFORE, in connection with an agreement 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 parties who have violated the relevant laws and regulations.

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

3. To support this critical obligation, the Cybersecurity Regulation places on all DFS-regulated entities ("Covered Entities"), including Travelers, an obligation to establish and implement a cybersecurity program, including the implementation of certain cybersecurity policies and procedures based on a Risk Assessment and designed to protect the confidentiality and integrity of its Information Systems, as well as any consumer NPI contained therein. 23 NYCRR §§ 500.1(c), 500.1(e), 500.1(g), 500.1(k), 500.2(b), 500.3.

4. To secure and protect customer NPI and prevent Cybersecurity Event(s), as defined in 23 NYCRR § 500.1(d), Covered Entities must limit user access privileges to Information Systems that provide access to NPI and shall "use effective controls, which may include Multi-Factor Authentication or Risk-Based Authentication, to protect against unauthorized access to NPI or Information Systems." 23 NYCRR §§ 500.7, 500.12(a).

Event at Issue

The ForAgents Cybersecurity Event

5. On January 28, 2021, the Department issued an informal alert to several regulated insurance entities, including Travelers, stating that the Department "received reports from several sources that cybercriminals are conducting a widespread campaign to steal data from insurance company websites offering instant online automobile insurance premium quotes that display partial or redacted consumer information, such as drivers' license numbers" (the "January Alert").

6. On February 16, 2021, the Department issued an industry letter, titled "Cyber Fraud Alert," warning the industry of a "systemic and aggressive campaign to exploit cybersecurity flaws in public-facing [instant quote] websites to steal NPI" (the "February Alert").[1]

7. After receiving these initial alerts, Travelers took steps to ensure drivers' license numbers ("DLNs") and other NPI were either already masked or to apply additional masking on certain public-facing instant quoting applications.

8. On March 30, 2021, the Department issued a follow-up industry letter to the February Alert, titled "Cyber Fraud Alert Follow-Up" warning that the threat actors' campaign to steal NPI through instant quote websites had expanded to include not only consumer-facing websites but also portals accessed by independent agents via credential stuffing attacks (the "March Alert"). Specifically, the March Alert stated, "[a]gent portals should be protected by the robust access controls required by DFS's cybersecurity regulation."[2]

[1] https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210216_cyber_fraud_alert.
[2] https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210330_cyber_alert_followup.

9. Following the March Alert, Travelers implemented additional controls designed to increase security on Travelers' web applications, including reviewing Travelers' applications for identification of potentially exposed NPI and beginning the process of deploying MFA on its agent portal, the ForAgents Portal.

10. Several months later, on November 15, 2021, The Travelers Indemnity Company reported a Cybersecurity Event to the Department as required by 23 NYCRR § 500.17(b). On November 11, 2021, Travelers' third-party pre-fill provider notified Travelers that there was a spike in household driver reports being accessed by one agency in California using Travelers' ForAgents Portal. Travelers confirmed the report was accurate on November 12, 2021.

11. The ForAgents Portal is an internally developed web-based application, which does not access Travelers' internal network, for use by Travelers' independent agents, and accessible by the agents' unique credentials. The ForAgents Portal is designed to assist Travelers' independent agents in accessing quotes and household driver reports. Travelers' independent agents input certain identifying information, such as names and addresses, for a consumer or client and then an application programming interface ("API") call is made from the ForAgents Portal to the third-party pre-fill provider. The third-party pre-fill provider verifies the inputted information and returns additional information to the application's interface, including DLNs, household driver reports, and other NPI.

12. After confirming the spike in household driver reports by the third-party pre-fill provider, on November 12, 2021, Travelers determined that the login credentials for two ForAgents Portal accounts had been compromised. The threat actor was able to access the ForAgents Portal and the API call to the third-party pre-fill provider to access approximately 40,000 household driver reports, which include consumer DLNs, dates of birth, insurance

history, and vehicle information for individuals in the consumers' household. On the same day, Travelers reset the two accounts and blocked IP addresses associated with the fraudulent activity on the two accounts.

13. On November 13, 2021, Travelers detected another unauthorized attempt to access customer and agent accounts using credentials obtained from unknown sources. There was no unauthorized access to household driver reports on this date. Travelers disabled and then reset the passwords of the impacted accounts.

14. Finally, on November 17, 2021, another two agent accounts were used to fraudulently access additional household driver reports. At that time, and for the first time since the initial spike was detected, Travelers disabled all household driver reporting capabilities from the ForAgents Portal.

15. Travelers reconfigured the application so that DLNs and dates of birth for drivers and household members were returned only in masked form (in both the actual reports and in the HTML code for the application), and the reporting function was re-enabled on November 23, 2021.

16. It was later determined that suspicious activity relating to the ForAgents Portal dated back to April 7, 2021.

17. At the time the unauthorized access to the ForAgents Portal was identified in November 2021 and since the ForAgents Portal went live, the access controls in place for the portal were a complex password policy and a contractual agreement with independent agents, which included a provision prohibiting agents from sharing credentials.

18. In light of the incident, Travelers provided several tens of thousands of consumers, including New Yorkers, with notice that their data may have been compromised, and offered those consumers credit monitoring for up to one year.

Policy and Compliance Weaknesses

19. The Cybersecurity Regulation imposes requirements on Covered Entities designed to ensure the protection of NPI stored and/or accessible through a Covered Entity's Information Systems.

20. Section 500.3 of the Cybersecurity Regulation requires that Covered Entities "implement and maintain a written policy or policies . . . setting forth the Covered Entity's policies and procedures for the protection of its Information Systems and [NPI] stored on those Information Systems. The cybersecurity policy shall be based on the Covered Entity's Risk Assessment and address" specific enumerated areas. Specifically, with respect to the protection of NPI, a Covered Entity's cybersecurity policy must address "(d) access controls and identity management . . . [and] (k) customer data privacy." 23 NYCRR § 500.03.

21. In addition to the policies and procedures required by Section 500.3, pursuant to Section 500.7 of the Cybersecurity Regulation, Covered Entities are required to limit user access privileges to Information Systems that provide access to NPI. Section 500.12(a) further requires that Covered Entities use effective controls to protect against unauthorized access to NPI.

22. Travelers' contracts with its independent agents state that access credentials can only be used by the individuals to whom they are assigned, and incorporates Travelers Systems Access and Use Terms, and other applicable Travelers policies and standards, which, in part, require users to maintain the confidentiality of their username and password.

23. Notwithstanding the limitations on sharing credentials in the terms of the contracts with the independent agents, the Department's investigation revealed that Travelers was aware that independent agents may have been using shared credentials to access the ForAgents Portal, in violation of 23 NYCRR § 500.3(d).

24. Further, Travelers was aware, via the March Alert, that threat actors were exploiting agent credentials to access agent instant quote portals to obtain consumer NPI. However, despite the Department's recommendation in the March Alert to implement multifactor authentication ("MFA") and other robust access controls, Travelers did not take steps to implement MFA on the ForAgents Portal until September 2021, and the process was not completed until well after the threat actors gained access to the ForAgents Portal in November 2021. The failure to limit user access privileges to the ForAgents portal before that time violated 23 NYCRR § 500.7.

25. The lack of MFA or other mitigating controls on the ForAgents Portal, together with the fact that Travelers was aware that its independent agents may have used shared credentials when accessing the ForAgents Portal, constituted a failure to use effective controls to protect against unauthorized access to NPI, in violation of 23 NYCRR § 500.12(a).

Violations of Law and Regulations

26. Travelers failed to ensure the proper implementation of its cybersecurity policies, in violation of 23 NYCRR § 500.3(d) & (k).

27. At the time of the Cyber Event, Travelers did not limit user access privileges to the ForAgents Portal as required by 23 NYCRR § 500.7.

28. At the time of the Cyber Event, Travelers failed to use effective controls to protect against unauthorized access to NPI reachable through the ForAgents portal, in violation of 23 NYCRR § 500.12(a).

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

SETTLEMENT PROVISIONS

Monetary Penalty

29. No later than ten (10) days after the Effective Date (as defined below) of this Consent Order, the Company shall pay a total civil monetary penalty pursuant to New York Financial Services Law § 408 to the Department in the amount of one million two hundred thousand dollars and 00/100 Cents ($1,200,000.00). The payment shall be in the form of a wire transfer in accordance with instructions provided by the Department.

30. The Company 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.

31. The Company 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.

32. In assessing a penalty for failures in Travelers' Cybersecurity Program and compliance with the Cybersecurity Regulation, the Department has taken into account factors that include, without limitation: the extent to which the entity has 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.

33. The Department acknowledges Travelers' cooperation throughout this investigation. The Department also recognizes and credits Travelers' ongoing efforts to remediate the shortcomings identified in this Consent Order. Among other things, Travelers has demonstrated its commitment to maintaining a robust cybersecurity program and to remediation by devoting significant financial and other resources to implementing MFA for independent agent access to the ForAgents Portal, thereby increasing the protection of the NPI accessible through the portal.

Remediation

34. Travelers shall continue to strengthen its controls to protect its Information Systems and consumers' NPI in accordance with the requirements of the Cybersecurity Regulation.

Access Controls and NPI Review

35. Within one-hundred and eighty (180) days of the Effective Date of this Consent Order, Travelers will conduct an internal review (the "Access Controls and NPI Review") of all Information Systems, including web-based applications, that store or provide access to NPI and are accessible to consumers or independent agents.

36. In performing the Access Controls and NPI Review, Travelers shall assess the effectiveness of all controls, including access controls, utilized by such Information Systems to protect NPI from unauthorized access and identify areas where controls warrant improvement. Within sixty (60) days of the completion of the Access Controls and NPI Review, Travelers shall submit to the Department a detailed Action Plan identifying risks, issues, or areas warranting improvement identified by the Access Controls and NPI Review and setting forth the steps

Travelers will take to address same (the "Action Plan"). The Department's approval of the Action Plan shall not be unreasonably withheld.

Full and Complete Cooperation

37. The Company commits and agrees that it will fully cooperate with the Department regarding all terms of this Consent Order.

Further Action by the Department

38. No further action will be taken by the Department against the Company or its successors for the conduct set forth in this Consent Order, 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.

39. Notwithstanding any other provision in 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 in connection with this matter.

Waiver of Rights

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

41. 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

42. 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

43. In the event that the Department believes the Company 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.

44. The Company 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 State Financial Services Law, Insurance Law, and any other applicable laws, and may use any evidence available to the Department in any ensuing hearings, notices, or orders.

Notices

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

For the Department:

Christopher J. Hummel
Senior Assistant Deputy Superintendent
Consumer Protection and Financial Enforcement Division
One Commerce Plaza, 20th Floor
Albany, New York 12257

Madeline W. Murphy
Deputy Director of Enforcement
Consumer Protection and Financial Enforcement Division
One Commerce Plaza, 20th Floor
Albany, New York 12257

For Travelers:

Christine Kucera Kalla
Executive Vice President and General Counsel
38 Washington Street
St. Paul, MN 55102

Miscellaneous

46. 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.

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

48. 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.

49. 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.

50. 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.

51. 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.

52. 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.

53. 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 Assistant Deputy Superintendent
Consumer Protection and Financial Enforcement

November 20, 2024

By: /s/ Madeline W. Murphy
MADELINE W. MURPHY
Deputy Director of Enforcement
Consumer Protection and Financial Enforcement

November 20, 2024

By: /s/ Christopher B. Mulvihill
CHRISTOPHER B. MULVIHILL
Deputy Superintendent for Consumer Protection and Financial Enforcement

November 20, 2024

By: /s/ Samantha R. Darche
SAMANTHA R. DARCHE
Acting Executive Deputy Superintendent for Consumer Protection and Financial Enforcement

November 20, 2024

TRAVELERS INDEMNITY COMPANY

By: /s/ Christine Kucera Kalla
Christine Kucera Kalla
Executive Vice President and General Counsel

November 8, 2024

THE FOREGOING IS HEREBY APPROVED. IT IS SO ORDERED.

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

November 25, 2024