ATTORNEY GENERAL OF THE STATE OF NEW YORK
BUREAU OF INTERNET & TECHNOLOGY

In the Matter of

Assurance No. 24-082

Investigation by LETITIA JAMES,
Attorney General of the State of New York, of

Government Employees Insurance Company,

Respondent.

ASSURANCE OF DISCONTINUANCE

The Office of the Attorney General of the State of New York ("OAG") commenced an investigation pursuant to Executive Law § 63(12) and General Business Law ("GBL") § 899-bb into a data security incident at Government Employees Insurance Company ("GEICO" or "Respondent"). This Assurance of Discontinuance ("Assurance") contains the findings of OAG's investigation and the relief agreed to by the OAG and GEICO whether acting through its respective directors, officers, employees, representatives, agents, affiliates, or subsidiaries (collectively, the "Parties").

FINDINGS OF OAG

1. Many automobile insurance companies provide a website for use by consumers and insurance agents to generate insurance quotes. These quoting tools are supplied with a data "prefill" capability. When a user enters basic personal details—such as name, date of birth, and/or address—a quote tool can automatically populate (or "prefill") other fields with additional personal information about the person. Quoting tools for consumers are available on the insurer's public website, and quoting tools for agents are available on agent-specific sites.

2. To provide prefill functionality, insurance companies contract with third-party data providers to license the use of the data providers' databases. These databases contain vast amounts of consumer data, including the private information of New York residents as defined by General Business Law ("GBL") §§ 899-aa and 899-bb. After a user enters their basic personal details into the instant quote application, the application transmits the information to the data provider. The data provider, in turn, uses that information to identify the consumer associated with those data points, and then returns additional data about the consumer to the insurer's instant quote application.

3. Depending on the type of data returned, the insurer can then use that data to populate prefill fields in the application. These automatically populated fields tend to include information that is relevant in estimating an auto insurance quote, but which the average consumer might not know from memory, including the consumer's driver's license number ("DLN") and vehicle identification number. These fields can also include names and DLNs of additional members of the consumer's household.

Threat Actors Obtained New Yorkers' Private Information Through Vulnerabilities in GEICO's Instant Quoting Tool

4. Respondent GEICO is a company headquartered in Maryland that engages in the automobile insurance business. It is licensed to sell insurance products to consumers in New York State.

5. As part of this business and at all relevant times, GEICO maintained a consumer-facing quoting application on its public website and a website with an online quoting tool for use by insurance agents.

6. GEICO's consumer-facing quoting application prompted users to enter their name, date of birth, and address. Not all data points needed to be accurate in order to trigger prefilling.

7. When a user triggered prefilling, DLNs were encrypted in transit from GEICO's third-party data provider to GEICO and through GEICO's systems, and partially masked on the face of the end user's browser. However, the consumer quoting tool exposed consumers' full DLNs in plaintext as the DLN was transmitted to the browser.

8. GEICO's consumer-facing quoting tool also exposed full DLNs in plaintext in responses to two API calls intended for agent-side use. One API function displayed queries from GEICO's prefill tool, and the other API function displayed queries from GEICO's customer lookup system. The URLs used to make the API calls were exposed in the code of its consumer-facing quoting tool.

9. On or around November 15, 2020, threat actors began targeting GEICO's consumer-facing quoting tool, triggering the prefill function to return plaintext DLNs of New York consumers and their household members. Threat actors were, over time, able to acquire more than 116,000 New Yorkers' DLNs in this manner.

10. On or around December 29, 2020, GEICO detected a spike in unfinished quotes on its quoting application.

11. On January 13, 2021, GEICO detected a pattern of individuals exiting the quote flow at the step where DLNs were prefilled.

12. On January 14, 2021, GEICO implemented an update that masked DLNs on its own servers.

13. On or around the same day, GEICO's cybersecurity team conducted a review of dark web forums, which showed that in late December 2020, threat actors were discussing obtaining DLNs from GEICO and offering "DL lookup" services or to sell "the GEICO method." GEICO's cybersecurity team also observed threat actors discussing "the GEICO method" on messaging channels.

14. A few days after GEICO masked DLNs on January 14, a user posted on a social media forum that "there is a new Geico method to get the dl."

15. On January 21, 2021, GEICO discovered a second point where DLNs were exposed in plaintext through its consumer-facing quoting tool. The same day, GEICO masked DLNs exposed at this second point. GEICO reported to the OAG the cybersecurity incident involving its consumer-facing quoting tool on February 1, 2021.

16. Meanwhile, starting on or around November 24, 2020, threat actors began exploiting the exposed APIs intended for agent use. Threat actors were able to make calls on APIs meant for agent use because those APIs were exposed on GEICO's consumer-facing quoting tool.

17. These APIs were exploited only sporadically until January 21, 2021, when GEICO successfully masked DLNs exposed through the prefilling function of its consumer-facing quoting tool. Starting January 22, 2021, malicious activity exploiting the exposed APIs increased significantly. On or about February 12, 2021, GEICO detected that the quote completion rate had significantly decreased but did not attribute the anomaly to the exposed APIs.

18. On January 27, 2021, GEICO discovered that threat actors were purchasing policies and filing fraudulent claims to gain access to consumers' DLNs. The next day, GEICO

deployed an update to prevent access to DLNs through this method. GEICO reported this cybersecurity incident to the OAG on February 23, 2021.

19. On January 28, 2021, GEICO received an email alert from the NY Department of Financial Services ("DFS"), warning that cyber attackers were conducting a widespread campaign to steal DLNs through insurance companies' quoting tools and that the DFS expected the attackers "will attempt a wide range of techniques" to steal non-public information.

20. On February 16, 2021, GEICO received another DFS alert that expanded upon the "systemic and aggressive campaign" to obtain private information that it had previously warned companies about in its January 28 email. The DFS warned of additional tactics threat actors were using to obtain DLNs and instructed regulated entities to review whether it was necessary to display any private information to users, even in redacted form.

21. Despite being aware of threat actor discussions on how to exfiltrate DLNs from GEICO, experiencing at least two different attacks on its consumer quoting tool to extract DLNs, and receiving repeated alerts from DFS corroborating a "systemic and aggressive campaign" to steal DLNs and warning of the threat actors' continuously evolving tactics and discovery of additional points of exposure, GEICO did not correctly identify activity on its API endpoints as threat actors exfiltrating DLNs.

22. Accordingly, GEICO never detected the malicious calls being made on its agent-side APIs. Rather, on March 1, 2021, a third party alerted GEICO to one of the exposed APIs, explaining that it could be exploited to retrieve plaintext DLNs. The same day, GEICO disabled the affected part of system.

23. On March 2, 2021, GEICO deployed a patch that blocked access to the first API's URL.

24. On March 4, 2021, GEICO discovered the second API and disabled it the same day.

25. GEICO reported the incident involving the exposed APIs to the OAG on April 16, 2021.

26. From the time threat actors began to exploit GEICO's quoting tool and exposed APIs until GEICO remediated the DLN exposures, threat actors were able to access and obtain approximately 135,414 DLNs, of which approximately 116,611 belonged to NY residents.

27. Many of the New York DLNs acquired as part of these attacks were subsequently used in fraudulent unemployment claims filed with the New York State Department of Labor ("DOL"). Although DOL identified many of these fraudulent claims prior to issuing any payments, thousands of fraudulent claimants received at least some amount of unemployment benefits issued in the name of the victims of these attacks.

GEICO Did Not Adopt Reasonable Safeguards to Protect Private Information

28. GEICO failed to adopt reasonable safeguards to protect the private information of New Yorkers that it licensed and used to provide quotes on its website.

29. As of the time of the incident, GEICO failed to protect DLNs used in connection with quote generation and customer lookup. DLNs were not included in the scope of GEICO's annual enterprise risk assessment.

30. In particular, GEICO failed:

a. to design its consumer quoting tool securely to ensure that it transmitted only DLNs that were masked;

b. to make agent-facing APIs inaccessible in the code of its consumer-facing quoting tool before deploying it to the public internet;

c. to monitor for suspicious activity on all API endpoints handling private information, even after becoming aware of threat actors' focus on DLNs;

d. to attribute the anomalous activities it observed to the misuse of its agent-facing APIs until a third party alerted GEICO to it more than three months after the attacks began and over a month after the attacks intensified.

31. After the incidents, GEICO implemented additional safeguards to protect consumer private information, including:

a. implementing, in April 2021, a previously planned new design for its online quoting application;

b. undertaking a company-wide evaluation of consumer-facing applications;

c. implementing additional alerting for anomalous behavior; and

d. implementing additional web application firewall blocks to prevent public access to agent-facing APIs.

GEICO's Conduct Violated New York Law

32. Executive Law § 63(12) prohibits illegal practices in the conduct of any business.

33. GBL § 899-bb requires any person or business that owns or licenses computerized data which includes the private information of a resident of New York to develop, implement, and maintain reasonable safeguards to protect the security, confidentiality, and integrity of the private information. "Private information" includes an individual's name in combination with their DLN. GBL § 899-aa(1)(b).

34. The OAG finds that Respondent's conduct violated Executive Law § 63(12) and GBL § 899-bb.

35. Respondent neither admits nor denies the OAG's Findings in paragraphs 1-34 above.

36. The OAG finds the relief and agreements contained in this Assurance appropriate and in the public interest. THEREFORE, the OAG is willing to accept this Assurance pursuant to Executive Law § 63(15), in lieu of commencing a statutory proceeding for violations of Executive Law § 63(12) and GBL § 899-bb based on the conduct described above.

IT IS HEREBY UNDERSTOOD AND AGREED, by and between the Parties:

RELIEF

37. For the purposes of this Assurance, the following definitions shall apply:

a. "API" means application programming interface.

b. "Network" means any networking equipment, databases, data stores, applications, software, servers, endpoints, or other equipment or services that are capable of using, exchanging, or sharing software, data, hardware, or other resources and that are owned and/or operated by or on behalf of Respondent.

c. "Private Information" means private information as defined in New York General Business Law § 899-aa(1)(b).

d. "Security Event" means unauthorized access to or acquisition of Private Information collected, used, stored, retrieved, transmitted, displayed, maintained, or otherwise processed by Respondent.

GENERAL COMPLIANCE

38. Respondent shall comply with Executive Law § 63(12) and GBL § 899-bb in connection with its collection, maintenance, use, and disclosure of Private Information.

INFORMATION SECURITY PROGRAM

39. Respondent shall maintain a comprehensive, written information security program ("Information Security Program") that is reasonably designed to protect the security, integrity, and confidentiality of Private Information that Respondent collects, maintains, uses, or discloses. The Information Security Program shall, at a minimum, include the information security requirements detailed in paragraphs 42-47 and the following processes:

a. Evaluate, update, and document, not less than annually, internal and external risks to the security, integrity and confidentiality of Private Information;

b. Design, implement, and maintain reasonable administrative, technical, and physical safeguards to control the internal and external risks Respondent identified that are appropriate to: (i) the size and complexity of Respondent's operations; (ii) the nature and scope of Respondent's activities; and (iii) the volume and sensitivity of the Private Information that Respondent collects, maintains, uses, or discloses;

c. Evaluate and document, not less than annually, the sufficiency of any safeguards in place to address the internal and external risks to Private Information Respondent identified, and modify the Information Security Program based on the results to ensure that the safeguards comply with Paragraph 39(b) above;

d. Test and monitor the effectiveness of such safeguards not less than annually, and modify the Information Security Program based on the results of testing and monitoring to ensure the safeguards comply with Paragraph 39(b) above; and

e. Evaluate the Information Security Program not less than annually, adjust the Program in light of any changes to Respondent's operations or business arrangements, or any other circumstances that Respondent knows or has reason to know may have an impact on the effectiveness of the Program, and document any adjustments.

f. With respect to third-party service providers, take reasonable steps to select service providers capable of reasonably safeguarding Private Information, contractually require service providers to implement and maintain reasonable safeguards to protect Private Information, and periodically evaluate the continued adequacy of service providers' cybersecurity practices.

40. Respondent shall employ a qualified employee responsible for implementing, maintaining, evaluating, updating, and monitoring the Information Security Program (the "Chief Information Security Officer"). The Chief Information Security Officer shall have the credentials, background, and expertise in information security appropriate to the level, size, and complexity of their role in implementing, maintaining evaluating, updating, and monitoring the Information Security Program. The Chief Information Security Officer shall report at least annually to Respondent's Board of Directors (or an appropriately designated Board Committee) or equivalent, or, in the absence of the foregoing, to a senior officer or officers responsible for Respondent's Information Security Program. Such reports shall be in writing and address issues including but not be limited to the sufficiency of resources allocated to the Information Security Program, the overall effectiveness of the Information Security Program, and any material cybersecurity risks.

41. Respondent shall provide notice of the requirements of this Assurance to its management-level employees responsible for implementing, maintaining, evaluating, updating, or monitoring the Information Security Program within sixty (60) days of the Effective Date of this Assurance or the date they assumed their responsibilities for implementing, maintaining, evaluating, updating, or monitoring the Information Security Program, whichever is later. Respondent shall document that it has provided the notices required in this paragraph.

SPECIFIC INFORMATION SECURITY REQUIREMENTS

42. Private Information Inventory: Within sixty (60) days of the Effective Date of this Assurance, Respondent shall:

(i) develop and maintain an inventory of all applications that collect, maintain, use, or disclose Private Information;

(ii) develop, implement, and maintain written policies and procedures designed to ensure its Private Information Inventory shall, at a minimum:

a. Identify all points at which such applications collect, maintain, use, or disclose Private Information;

b. Map and/or track the complete path of all data flows involving Private Information, including API calls, emanating from or ending at such applications; and

c. Ensure that reasonable safeguards are used to protect Private Information at all times, including but not limited to appropriate encryption, masking, obfuscation, and other methods of rendering Private Information incomprehensible and/or inaccessible, or other alternative compensating controls reviewed and approved by the Chief Information Security Officer;

d. Be evaluated, updated, and documented not less than annually; and

(iii) negotiate with the OAG a reasonable timeline within which Respondent shall implement its Private Information Inventory.

In the event Respondent is unable to meet the agreed-upon deadline, it shall notify the OAG at least thirty (30) days before the deadline to request an extension, which the OAG shall not unreasonably withhold.

43. Governance: Respondent shall maintain reasonable written policies and procedures designed to ensure the security, integrity, and confidentiality of Private Information obtained from a third party.

44. Secure Software Development Lifecycle: Respondent shall maintain written policies and procedures designed to ensure secure software development lifecycle practices for web-based, mobile, or other applications—whether public-facing, credential-based, or internal—maintained by or on behalf of Respondent that collect, maintain, use, or disclose Private Information. Such policies and procedures must include the following:

a. For applications developed or maintained in-house, wherever Private Information is implicated by the regular and expected use of any such application, Respondent shall consider the privacy impact throughout the software development lifecycle, including software maintenance and testing.

b. For in-house software development personnel, provide periodic education on Private Information, how such information can be used for fraud, and Respondent's procedures, guidelines, and standards for protecting such information;

c. For applications developed by a service provider, comply with Paragraph 39(f) of this Assurance.

45. Authentication Policy and Procedures: Respondent shall maintain reasonable authentication procedures for access to Respondent's information systems that provide access to Private Information.

46. Logging & Monitoring: Respondents shall develop, implement, and maintain a system designed to collect and monitor Network activity, such as through security and event management tools, as well as reasonable policies and procedures designed to properly configure such tools to report anomalous activity. The system shall, at a minimum: (i) provide for centralized logging and monitoring that includes collection and aggregation of logging for any platforms or applications operated by or on behalf of Respondent that collect, maintain, use, or disclose Private Information, and (ii) monitor for and alert security personnel to suspicious activity. Logs should be readily accessible for a period of at least ninety (90) days and stored for at least one year from the date the activity was logged.

47. Threat Response: Whenever Respondent is aware of a Security Event, Respondent shall:

a. Promptly monitor for indicators of additional attacks exploiting similar vulnerabilities, leveraging similar tactics, techniques, and procedures, or targeting the same type of Private Information;

b. Promptly conduct a reasonable investigation to determine, at a minimum, whether Private Information is exposed or otherwise at risk; and

c. Promptly implement changes necessary to protect Private Information at risk.

OAG ACCESS TO RECORDS

48. Respondent shall retain the documentation and reports required by paragraphs 39-42 for at least six years. Such documentation and reports shall be made available to the OAG within fourteen (14) days of a written request from the OAG. For avoidance of doubt, this paragraph does not require Respondent to provide the OAG with copies of any draft documents, draft reports, or communications that would otherwise be protected as attorney work product or under the attorney-client privilege.

MONETARY RELIEF

49. Respondent shall pay to the State of New York four million seven hundred and fifty thousand dollars ($4,750,000) in civil penalties. Payment shall be made in full within thirty (30) business days of the Effective Date of this Assurance. Any payment shall reference AOD No. 24-082.

MISCELLANEOUS

50. Respondent expressly agrees and acknowledges that the OAG may initiate a subsequent investigation, civil action, or proceeding to enforce this Assurance, for violations of the Assurance, or if the Assurance is voided pursuant to paragraph 56, and agrees and acknowledges that in such event:

a. Any statute of limitations or other time-related defenses are tolled from and after the effective date of this Assurance;

b. the OAG may use statements, documents or other materials produced or provided by the Respondent prior to or after the Effective Date of this Assurance;

c. any such civil action or proceeding must be adjudicated by the courts of the State of New York, and that Respondent irrevocably and unconditionally waives any objection based upon personal jurisdiction, inconvenient forum, or venue; and

d. evidence of a violation of this Assurance shall constitute prima facie proof of a violation of the applicable law pursuant to Executive Law § 63(15).

51. If a court of competent jurisdiction determines that the Respondent has violated this Assurance, the Respondent shall pay to the OAG the reasonable cost, if any, of obtaining such determination and of enforcing this Assurance, including, without limitation, legal fees, expenses, and court costs.

52. Acceptance of this Assurance by the OAG is not an approval or endorsement by the OAG of any of Respondent's policies, practices, or procedures, and the Respondent shall make no representation to the contrary.

53. All terms and conditions of this Assurance shall continue in full force and effect on any successor, assignee, or transferee of the Respondent. Respondent shall include in any such successor, assignment, or transfer agreement a provision that binds the successor, assignee, or transferee to the terms of the Assurance. No party may assign, delegate, or otherwise transfer any of its rights or obligations under this Assurance without the prior written consent of the OAG.

54. Any failure by the OAG to insist upon the strict performance by Respondent of any of the provisions of this Assurance shall not be deemed a waiver of any of the provisions hereof, and the OAG, notwithstanding that failure, shall have the right thereafter to insist upon

the strict performance of any and all of the provisions of this Assurance to be performed by the Respondent for the duration of such provision.

55. All notices, reports, requests, and other communications pursuant to this Assurance must reference Assurance No. 24-082, and shall be in writing and shall, unless expressly provided otherwise herein, be given by hand delivery, express courier, or electronic mail at an address designated in writing by the recipient, followed by postage prepaid mail, and shall be addressed as follows:

> If to the Respondent, to: GEICORegulatoryNotices@geico.com, care of Tracey Laws or in their absence, to the person holding the title of Head of Government and Regulatory Affairs.
>
> If to the OAG, to Gena Feist, Assistant Attorney General, or in her absence, to the person holding the title of Bureau Chief.
>
> Bureau of Internet & Technology
> 28 Liberty Street
> New York, NY 10005

56. The OAG has agreed to the terms of this Assurance based on, among other things, the representations made to the OAG by the Respondent and their counsel and the OAG's own factual investigation as set forth in Findings in paragraphs 1-34 above. The Respondent represents and warrants that neither it nor its counsel has made any material representations to the OAG that are inaccurate or misleading. If any material representations by Respondent or its counsel are later found to be inaccurate or misleading, this Assurance is voidable by the OAG in its sole discretion.

57. No representation, inducement, promise, understanding, condition, or warranty not set forth in this Assurance has been made to or relied upon by the Respondent in agreeing to this Assurance.

58. The Respondent represents and warrants, through the signatures below, that the terms and conditions of this Assurance are duly approved. Respondent further represents and warrants that GEICO, by Tangela Richter, as the signatory to this AOD, is a duly authorized officer acting at the direction of the Board of Directors of GEICO.

59. Nothing in this Agreement shall relieve Respondent of other obligations imposed by any applicable state or federal law or regulation, or other applicable law.

60. Respondent shall not take any action or make any statement denying, directly or indirectly, the propriety of this Assurance, or expressing the view that this Assurance is without factual basis. Nothing in this paragraph affects Respondent's (i) testimonial obligations or (ii) right to take legal or factual positions in defense of litigation or other legal proceedings to which the OAG is not a party. This Assurance is not intended for use by any third party in any other proceeding.

61. Nothing contained herein shall be construed to limit the remedies available to the OAG in the event that the Respondent violates the Assurance after its effective date.

62. This Assurance may not be amended except by an instrument in writing signed on behalf of the Parties to this Assurance.

63. In the event that any one or more of the provisions contained in this Assurance shall for any reason be held by a court of competent jurisdiction to be invalid, illegal, or unenforceable in any respect, in the sole discretion of the OAG, such invalidity, illegality, or unenforceability shall not affect any other provision of this Assurance.

64. Respondent acknowledges that they have entered this Assurance freely and voluntarily and upon due deliberation with the advice of counsel.

65. This Assurance shall be governed by the laws of the State of New York without regard to any conflict of laws principles.

66. The Assurance and all its terms shall be construed as if mutually drafted with no presumption of any type against any party that may be found to have been the drafter.

67. This Assurance may be executed in multiple counterparts by the parties hereto. All counterparts so executed shall constitute one agreement binding upon all parties, notwithstanding that all parties are not signatories to the original or the same counterpart. Each counterpart shall be deemed an original to this Assurance, all of which shall constitute one agreement to be valid as of the effective date of this Assurance. For purposes of this Assurance, copies of signatures shall be treated the same as originals. Documents executed, scanned, and transmitted electronically and electronic signatures shall be deemed original signatures for purposes of this Assurance and all matters related thereto, with such scanned and electronic signatures having the same legal effect as original signatures.

68. The effective date of this Assurance shall be the date that it is signed by the OAG.

LETITIA JAMES
Attorney General of the State of New York
28 Liberty Street
New York, NY 10005

By: _____
Gena Feist
Assistant Attorney General
Bureau of Internet & Technology

Date: 11/21/24

Government Employees Insurance Company
5260 Western Avenue
Chevy Chase, Md. 20815

By: Tangela Richter
Tangela Richter
Chief Legal Officer

Date: November 4, 2024

ATTORNEY GENERAL OF THE STATE OF NEW YORK
BUREAU OF INTERNET & TECHNOLOGY

In the Matter of Assurance No. 24-091

Investigation by LETITIA JAMES,
Attorney General of the State of New York, of

The Travelers Indemnity Company,

Respondent.

ASSURANCE OF DISCONTINUANCE

The Office of the Attorney General of the State of New York ("OAG") commenced an investigation pursuant to Executive Law § 63(12) and General Business Law ("GBL") § 899-bb into a data security incident at The Travelers Indemnity Company ("Travelers" or "Respondent"). This Assurance of Discontinuance ("Assurance") contains the findings of the OAG's investigation and the relief agreed to by the OAG and Travelers (collectively, the "Parties"), whether Travelers is acting through its respective directors, officers, employees, representatives, agents, affiliates, or subsidiaries.

FINDINGS OF OAG

1. Many automobile insurance companies provide a website for use by consumers and insurance agents to generate insurance quotes. These quoting tools are supplied with a data "prefill" capability. When a user enters certain personal details—such as name, date of birth, and/or address—a quote tool with prefill capabilities can automatically populate (or "prefill") other fields with additional personal information about the person. Quoting tools for consumers are available on the insurer's public website, and quoting tools for agents are available on agent-

specific sites that require credentials to access.

2. To provide prefill functionality, insurance companies contract with third-party data providers to license the use of the data provider's databases. These databases contain vast amounts of consumer data, including the private information of New York residents as defined by General Business Law ("GBL") §§ 899-aa and 899-bb. After a user enters the required data points into the instant quote application, the application transmits the information to the data provider. The data provider, in turn, uses that information to identify the consumer associated with those data points, and then returns additional data about the consumer to the insurer's instant quote application.

3. Depending on the type of data returned, the insurer can then use that data to populate prefill fields in the application. These automatically populated fields tend to include information that is relevant in estimating an auto insurance quote, but which the average consumer might not know from memory, including the consumer's driver's license number ("DLN") and vehicle identification number These fields can also include names and DLNs of additional members of the consumer's household.

Travelers' ForAgents Portal

4. Respondent is a company incorporated in Connecticut with its headquarters in Hartford, CT. Among other activities, Travelers engages in the automobile insurance business. It is licensed to sell insurance products to consumers in New York State.

5. As part of this business and at all relevant times, Travelers maintained a consumer-facing quoting application on its public website and a portal with an online quoting tool for use by independent insurance agents ("ForAgents Portal" or "Portal"). Access to the Portal required a username and password

6. Through the ForAgents Portal, independent insurance agents were able to access the quoting tool and generate household driver reports that contained DLNs populated by the prefill functionality. In addition to the subject consumer's DLN, the household driver reports also included the DLNs of any other drivers in the subject consumer's household. The DLNs in these reports were not truncated or masked.

7. Tens of thousands of independent insurance agents nationwide used the ForAgents Portal. Despite such widespread access and the ready availability of consumer private information in plaintext to any user of the Portal, Travelers secured the ForAgents Portal by only username and password, without multi-factor authentication ("MFA"). Travelers did not further protect the ForAgents Portal until November 2021, when it discovered that its ForAgents Portal had been breached

8. Prior to November 2021, Travelers monitored household driver report generation only at an aggregate level, not at the agent level. Thus, if a particular agent had an abnormal spike in reports, such a spike might go unnoticed if the activity did not rise to a level that noticeably impacted aggregate metrics.

Industry Cybersecurity Alerts

9. Beginning in late January 2021, the New York State Department of Financial Services ("DFS") issued a number of alerts concerning a series of cyberattacks targeting insurers that maintained online quoting tools.

a. On January 28, 2021, DFS distributed an email alert to insurance companies, warning that online threat actors were exploiting instant quote applications available on consumer-facing websites to obtain consumer private information such as DLNs. DFS noted that it expected the threat actors to "attempt a wide range of

techniques" to obtain DLNs and identified two confirmed ways in which private information was being exposed through quoting tools—in the website HTML and network traffic.

b. On February 16, 2021, DFS issued an industry letter to all of its regulated entities, including all licensed insurance companies, expanding upon the "systemic and aggressive campaign to exploit cybersecurity flaws" to obtain private information, which it had previously warned companies about in its January 28, 2021 email. DFS warned of additional tactics the threat actors were using to obtain DLNs: policy purchase to access post-purchase documents containing DLNs and social engineering of insurance agents. DFS instructed regulated entities to review whether it was necessary to display any private information to users, even in redacted form.

c. On March 30, 2021, DFS issued another industry letter to all regulated entities, advising the industry that threat actors were also "aggressively target[ing]" portals meant for insurance agents and were using credential stuffing attacks to gain access to insurance agents' accounts. DFS advised that agent portals should be protected by robust access controls and should not provide access to consumer private information beyond what was strictly necessary for agents' business.

d. On April 19, 2021, DFS issued yet another industry alert concerning the "ongoing cybercrime campaign to steal New York State residents' drivers' license numbers (DLNs) from automobile insurers." DFS identified another tactic threat actors had discovered to obtain DLNs: from the bar codes of insurance ID cards provided after policy purchase.

10. Travelers received all of DFS' alerts concerning the cyber campaign targeting insurers for consumer DLNs.

11. Prior to the January 28, 2021 alert, Travelers had been investigating unusual traffic patterns on its consumer-facing instant quote tool. Travelers discovered many fraudulent quote attempts, but because Travelers had masked DLNs server-side, threat actors had been unable to intercept DLNs through the consumer-facing quote tool.

12. Prior to the February 16, 2021 alert, Travelers discovered that in a small number of cases, threat actors had purchased a policy and created a customer account, which exposed unmasked DLNs in the source code. This resulted in a handful of New York DLN compromises. Travelers canceled the fraudulently purchased policies, disabled the fraudulently created accounts, masked DLNs in the source code of customer accounts, and notified impacted individuals.

13. Despite having detected two different attacks on its consumer-facing quoting tool and receiving multiple industry alerts corroborating a "systemic and aggressive campaign" to steal DLNs and warning of the threat actors' continuously evolving tactics and discovery of additional points of exposure, Travelers did not promptly act to further protect the full, plaintext DLNs available on the ForAgents Portal, such as by partially masking them.

14. After receiving the March 30, 2021 alert specifically warning that threat actors were aggressively targeting agent portals through credential stuffing attacks, Travelers reviewed, but did not change, its password policy. At the time, Travelers required passwords to be 8-15 alphanumeric upper- and lower-case characters, not be the same as the username or the word "password," and not contain more than two repeating characters. Passwords expired every 90 days, accounts were locked after 10 incorrect password attempts, and users could not use their

last six passwords.

The ForAgents Portal Compromise

15 Starting on or around April 7, 2021—one week after DFS' March 30, 2021 alert warning that threat actors had started aggressively targeting agent portals with credential stuffing attacks—threat actors gained access to the ForAgents Portal using compromised credentials. In total, threat actors generated approximately 40,000 household driver reports to obtain New Yorkers' DLNs.

16. Travelers did not detect any of these compromises.

17. More than seven months later, on November 11, 2021, Travelers was notified by its third-party prefill provider of a spike in the volume of household driver reports being accessed by one agency.

18. On November 12, 2021, Travelers identified two agent accounts had been compromised and, on the same day, reset the two agent accounts and blocked IP addresses associated with fraudulent activity on those two accounts.

19. On November 13, 2021, Travelers detected additional attempts to gain unauthorized access to customer and agent accounts. Travelers disabled the accounts that were successfully breached and reset the passwords of accounts that were targeted but not successfully breached.

20. On November 17, 2021, Travelers identified another two agent accounts that had been compromised and were accessing reports without authorization. That day, Travelers disabled all household driver reporting capabilities on the ForAgents Portal, cutting off access to consumers' DLNs via the ForAgents Portal.

21. On November 23, 2021, nearly eight months after DFS had warned Travelers that threat actors were obtaining unauthorized access to agent portals, Travelers re-enabled the

household reporting function on the ForAgents Portal after reconfiguring its reporting tool so that DLNs in household reports were masked, in both the actual reports and in the HTML code.

22. From the time that attackers began to exploit the ForAgents Portal on April 7, 2021, until Travelers effectively foreclosed the ability to access additional DLNs by disabling household reporting capabilities on November 17, 2021, attackers were able to access and obtain 88,858 consumers' DLNs without authorization, of which 3,912 were New Yorkers' DLNs.

23. Many of the New York DLNs acquired as part of these attacks were subsequently used in fraudulent unemployment claims filed with the New York State Department of Labor ("DOL") Although DOL identified many of these fraudulent claims prior to issuing any payments, some fraudulent claimants received at least some amount of unemployment benefits issued in the name of the victims.

24. After containing the ForAgents incident in November 2021, Travelers expedited implementation of various security enhancements it had been pursuing before it became aware of the ForAgents incident. In August 2021, Travelers had decided to enhance monitoring on the ForAgents Portal to allow visibility into report generation and access at the individual agent level. In September 2021, Travelers had engaged a bot management vendor to enhance controls on the ForAgents login page. And in October 2021, Travelers had begun the process of implementing MFA on the ForAgents Portal. In the wake of the ForAgents incident, Travelers expedited implementation of these projects, implementing the bot defense tool on the ForAgents login page on November 15, 2021, achieving full implementation of enhanced monitoring on November 18, 2021, and starting to roll out MFA to independent agents in the first quarter of 2022.

Travelers' Violations

25. Executive Law § 63(12) prohibits illegal practices in the conduct of any business

26. GBL § 899-bb requires any person or business that owns or licenses computerized data which includes the private information of a resident of New York to develop, implement, and maintain reasonable safeguards to protect the security, confidentiality, and integrity of the private information. "Private information" includes an individual's name in combination with their DLN. GBL §§ 899(bb)(1)(b), 899-aa(1)(b).

27. The OAG finds that Respondent's conduct violated Executive Law § 63(12) and GBL § 899-bb.

28. Respondent neither admits nor denies the OAG's Findings, paragraphs 1-27 above.

29. The OAG finds the relief and agreements contained in this Assurance appropriate and in the public interest. THEREFORE, the OAG is willing to accept this Assurance pursuant to Executive Law § 63(15), in lieu of commencing a statutory proceeding for violations of Executive Law § 63(12) and GBL § 899-bb based on the conduct described above.

IT IS HEREBY UNDERSTOOD AND AGREED, by and between the Parties:

RELIEF

30. For the purposes of this Assurance, the following definitions shall apply:

a. "Network" means any networking equipment, databases, data stores, applications, software, servers, endpoints, or similar equipment or services that: (i) are capable of using, exchanging, or sharing software, data, hardware, or other resources, (ii) are owned and/or operated by or on behalf of Respondent, and (iii) collect, use, store, retrieve, transmit, display, maintain and/or otherwise process Private Information.

b. "Private Information" means private information as defined in New York General Business Law § 899-aa(1)(b).

c. "Security Event" means unauthorized access to or acquisition of Private Information collected, used, stored, retrieved, transmitted, displayed, maintained, or otherwise processed by Respondent.

GENERAL COMPLIANCE

31. Respondent shall comply with Executive Law § 63(12) and GBL § 899-bb in connection with its collection, use, storage, retrieval, transmittal, display, maintenance, and other processing of Private Information.

INFORMATION SECURITY PROGRAM

32. Respondent shall, to the extent it has not already done so, maintain a comprehensive information security program ("Information Security Program" or "Program") that is reasonably designed to protect the security, integrity, and confidentiality of Private Information that Respondent collects, uses, stores, retrieves, transmits, displays, maintains and/or otherwise processes Respondent shall document in writing the content, implementation, and maintenance of the Information Security Program. The Information Security Program shall, at a minimum, include all of the requirements detailed in paragraphs 35- 40 and the following processes:

a. Assess, update as appropriate, and document, not less than annually, internal and external risks to the security, integrity and confidentiality of Private Information, including but not limited to all entries in the most recent Data Inventory;

b. Design, implement, and maintain reasonable administrative, technical, and physical safeguards to control the internal and external risks Respondent identified that

are appropriate to: (i) the size and complexity of Respondent's operations; (ii) the nature and scope of Respondent's activities; and (iii) the volume and sensitivity of the Private Information that Respondent collects, uses, stores, retrieves, transmits, displays, maintains and/or otherwise processes;

c. Assess, update as appropriate, and document, not less than annually, the sufficiency of any safeguards in place to address the internal and external risks to Private Information Respondent identified, and modify the Information Security Program based on the results to ensure that the safeguards comply with this Assurance;

d. Test and monitor the effectiveness of such safeguards not less than annually, and modify the Information Security Program based on the results to ensure the safeguards comply with this Assurance;

e. With respect to third-party service providers, take reasonable steps (which may vary based on the third-party and service provided) to: select service providers capable of reasonably safeguarding Private Information, contractually require service providers to implement and maintain reasonable safeguards to protect Private Information, and periodically evaluate the continued adequacy of service providers' cybersecurity practices; and

f. Assess, update as appropriate, and document, not less than annually, the Information Security Program and adjust the Program in light of any changes to Respondent's operations or business arrangements, or any other circumstances that Respondent knows or has reason to know may have an impact on the effectiveness of the Program.

33. Respondent shall, to the extent it has not already done so, designate a qualified employee responsible for implementing, maintaining, assessing, updating, and monitoring the Information Security Program (the "Chief Information Security Officer") The Chief Information Security Officer shall have the credentials, background, and expertise in information security appropriate to the level, size, and complexity of their role in implementing, maintaining, assessing, updating, and monitoring the Information Security Program. The Chief Information Security Officer shall report at least quarterly to Respondent's Chief Executive Officer (or the equivalent thereof) and at least semi-annually to the Board of Directors (or an appropriately designated Board Committee) concerning Respondent's Information Security Program. Such reports shall be in writing and include (as relevant) but not be limited to the following: the staffing and budgetary sufficiency of the Information Security Program; a status update on Respondent's Information Security Program, including any gaps in implementation and enforcement; any existing and emerging material security risks faced by Respondent; and any challenges to the success of the Information Security Program.

34. Within sixty (60) days of the Effective Date of this Assurance, Respondent shall provide notice of the requirements of this Assurance to its management-level employees responsible for implementing, maintaining, assessing, updating, or monitoring the Information Security Program. For a period of six (6) years following the Effective Date of this Assurance, Respondent shall annually train its management-level employees responsible for implementing, maintaining, assessing, updating, or monitoring the Information Security Program on the requirements of this Assurance and how to comply. Respondent shall document that it has provided the notices and training required in this paragraph.

SPECIFIC INFORMATION SECURITY REQUIREMENTS

35. Data Inventory: Within sixty (60) days of the Effective Date of this Assurance, Respondent shall: (a) review all instances in which it provides access to Private Information, (b) evaluate whether the controls in place reasonably ensure that access to Private Information is limited to the minimum level necessary, (c) consider whether any mitigating controls are appropriate to protect access to such Private Information, and, (d) implement such mitigating controls within a reasonable time period, not to exceed ninety (90) days from the date the appropriateness of such control was identified. Respondent shall review, update, and document its provision of access to Private Information not less than annually.

36. Governance: Respondent shall, to the extent it has not already done so, maintain reasonable written policies and procedures designed to ensure the security, integrity, and confidentiality of Private Information.

37. Authentication: By November 1, 2025, Respondent shall, to the extent it has not already done so, maintain reasonable account management and authentication procedures, including the use of MFA (or a reasonably equivalent control) for access to Private Information or remote access to Respondent's Network.

38. Monitoring: Respondent shall, to the extent it has not already done so, within 180 days, maintain a system(s) reasonably designed to collect and monitor activity on Respondent's Network (including with respect to third-party service providers, complying with paragraph 32(e) above). Respondent's system(s) shall, at a minimum and as appropriate: (a) provide for centralized logging and monitoring that includes collection and aggregation of logging for platforms or applications operated by or on behalf of Respondent that collect, maintain, use, or disclose Private Information on Respondent's Network (or a reasonably equivalent control), and

(b) monitor for and alert security personnel to suspicious activity. Logs on Respondent's centralized logging system should be immediately accessible (e.g., hot storage) for a period of at least 90 days and stored for at least one year from the date the activity was logged. Respondent shall also establish and maintain reasonable policies and procedures designed to properly configure such system(s) to alert on suspicious activity.

39. Threat Response: Whenever Respondent is aware of or reasonably should be aware of a reasonable risk of a Security Event, Respondent shall, to the extent it does not already do so, implement procedures to:

a Promptly monitor (or with respect to a third-party service provider, complying with paragraph 32(e) above) for suspicious activity on its Network that collect, use, store, retrieve, transmit, display, maintain, or otherwise process Private Information as needed to address such risk; monitoring shall be at a level that is sufficiently granular to detect a potential Security Event (where feasible);

b. Promptly conduct a reasonable investigation to determine, at a minimum, whether Private Information is exposed or otherwise at risk; and

c. Promptly implement changes necessary to protect Private Information at risk.

OAG ACCESS TO RECORDS

40. Respondent shall retain the documentation and reports required by paragraphs 32, 33, 34 and 35 for at least six years. Such documentation and reports shall be made available to the OAG within fourteen (14) days of a written request from the OAG. For avoidance of doubt, this paragraph does not require Respondent to provide the OAG with copies of any draft documents, draft reports, or communications that are or would otherwise be protected as attorney

work product or under the attorney-client privilege

MONETARY PENALTY

41. Respondent shall pay to the State of New York three hundred and fifty thousand dollars ($350,000) in civil penalties. Payment of the civil penalty shall be made in full by wire transfer within ten (10) business days of the Effective Date of this Assurance. Any payment shall reference Assurance No. 24-091.

MISCELLANEOUS

42 Respondent expressly agrees and acknowledges that the OAG may initiate a subsequent investigation, civil action, or proceeding to enforce this Assurance, for violations of the Assurance, or if the Assurance is voided pursuant to paragraph 49, and agrees and acknowledges that in such event:

a. any statute of limitations or other time-related defenses are tolled from and after the Effective Date of this Assurance;

b. the OAG may use statements, documents or other materials produced or provided by the Respondent prior to or after the Effective Date of this Assurance;

c. any civil action or proceeding must be adjudicated by the courts of the State of New York, and that Respondent irrevocably and unconditionally waives any objection based upon personal jurisdiction, inconvenient forum, or venue.

d. evidence of a violation of this Assurance shall constitute prima facie proof of a violation of the applicable law pursuant to Executive Law § 63(15).

43. If a court of competent jurisdiction determines that the Respondent has violated the Assurance, the Respondent shall pay to the OAG the reasonable cost, if any, of obtaining

such determination and of enforcing this Assurance, including without limitation legal fees, expenses, and court costs.

44. This Assurance is not intended for use by any third party in any other proceeding. This Assurance is not intended, and should not be construed, as an admission of liability by Respondent.

45 Acceptance of this Assurance by the OAG is not an approval or endorsement by OAG of any of Respondent's policies, practices, or procedures, and the Respondent shall make no representation to the contrary.

46. All terms and conditions of this Assurance shall continue in full force and effect on any successor, assignee, or transferee of the Respondent. Respondent shall include any such successor, assignment or transfer agreement a provision that binds the successor, assignee or transferee to the terms of the Assurance. No party may assign, delegate, or otherwise transfer any of its rights or obligations under this Assurance without the prior written consent of the OAG.

47. Any failure by the OAG to insist upon the strict performance by Respondent of any of the provisions of this Assurance shall not be deemed a waiver of any of the provisions hereof, and the OAG, notwithstanding that failure, shall have the right thereafter to insist upon the strict performance of any and all of the provisions of this Assurance to be performed by the Respondent.

48. All notices, reports, requests, and other communications pursuant to this Assurance must reference Assurance No. 24-091, and shall be in writing and shall, unless expressly provided otherwise herein, be given by hand delivery; express courier; or electronic

mail at an address designated in writing by the recipient, followed by postage prepaid mail, and shall be addressed as follows:

> If to the Respondent, to Christine Kucera Kalla, Executive Vice President and General Counsel, or in her absence, to the person holding the title of General Counsel.
>
> Travelers
> Attn: Christine Kucera Kalla
> 38 Washington Street
> St Paul, MN 55102
>
> If to the OAG, to Gena Feist, Assistant Attorney General, or in her absence, to the person holding the title of Bureau Chief.
>
> Bureau of Internet & Technology
> 28 Liberty Street
> New York, NY 10005

49. The OAG has agreed to the terms of this Assurance based on, among other things, the representations made to the OAG by the Respondent and their counsel and the OAG's own factual investigation as set forth in Findings, paragraphs 1- 27 above. The Respondent represents and warrants that neither it nor its counsel has made any material representations to the OAG that are inaccurate or misleading. If any material representations by Respondent or its counsel are later found to be inaccurate or misleading, this Assurance is voidable by the OAG in its sole discretion.

50. No representation, inducement, promise, understanding, condition, or warranty not set forth in this Assurance has been made to or relied upon by the Respondent in agreeing to this Assurance.

51. The Respondent represents and warrants, through the signatures below, that the terms and conditions of this Assurance are duly approved. Respondent further represents and

warrants that Travelers, by Christine Kucera Kalla, as the signatory to this Assurance, is a duly authorized officer acting at the direction of the Board of Directors of Travelers.

52. Nothing in this Assurance shall relieve Respondent of other obligations imposed by any applicable state or federal law or regulation or other applicable law.

53. Respondent agrees not to take any action or to make or permit to be made any public statement denying, directly or indirectly, any finding in the Assurance or creating the impression that the Assurance is without legal or factual basis. Nothing in this paragraph affects Respondent's right to take legal or factual positions in defense of litigation or other legal proceedings to which the OAG is not a party.

54 Nothing contained herein shall be construed to limit the remedies available to the OAG in the event that the Respondent violates the Assurance after its Effective Date.

55. This Assurance may not be amended except by an instrument in writing signed on behalf of the Parties to this Assurance.

56. In the event that any one or more of the provisions contained in this Assurance shall for any reason be held by a court of competent jurisdiction to be invalid, illegal, or unenforceable in any respect, in the sole discretion of the OAG, such invalidity, illegality, or unenforceability shall not affect any other provision of this Assurance.

57. Respondent acknowledges that they have entered this Assurance freely and voluntarily and upon due deliberation with the advice of counsel.

58. This Assurance shall be governed by the laws of the State of New York without regard to any conflict of laws principles.

59. The Assurance and all its terms shall be construed as if mutually drafted with no presumption of any type against any party that may be found to have been the drafter.

60. This Assurance may be executed in multiple counterparts by the parties hereto. All counterparts so executed shall constitute one agreement binding upon all parties, notwithstanding that all parties are not signatories to the original or the same counterpart. Each counterpart shall be deemed an original to this Assurance, all of which shall constitute one agreement to be valid as of the Effective Date of this Assurance. For purposes of this Assurance, copies of signatures shall be treated the same as originals. Documents executed, scanned and transmitted electronically and electronic signatures shall be deemed original signatures for purposes of this Assurance and all matters related thereto, with such scanned and electronic signatures having the same legal effect as original signatures.

61. The Effective Date of this Assurance shall be the date the OAG signs this Assurance.

LETITIA JAMES
Attorney General of the State of New York
28 Liberty Street
New York, NY 10005

By: _____
Gena Feist
Assistant Attorney General
Bureau of Internet & Technology

Date: 11/21/24

THE TRAVELERS INDEMNITY COMPANY
38 Washington Street
St. Paul, MN 55102

By: _____
Christine Kucera Kalla
Executive Vice President and General Counsel

Date: 11/21/24