

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

In the Matter of

Assurance No. 25-009

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

ROOT 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 Root Insurance Company (“Root” or “Respondent”). This Assurance of Discontinuance (“Assurance”) contains the findings of OAG’s investigation and the relief agreed to by the OAG and Root 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 to generate insurance quotes. These quoting tools are designed with a data “prefill” capability to pull in additional information about the individual from third party databases. When a user enters certain personal details—such as name, date of birth, and/or address—a quote tool with prefill capabilities will populate other fields with additional private information about the person. Quoting tools for consumers are available on the insurer’s public website.

2. To provide prefill functionality, insurance companies contract with third-party data providers to license the use of the data provider's information. 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 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 individual associated with those data points, and then returns additional data about the individual to the insurer's instant quote application.

3. These automatically populated fields include information that is relevant in estimating an auto insurance quote, but which the average consumer might not know from memory. Two common examples of pre-fill information are the consumer's driver's license number ("DLN") and vehicle identification number. Automatically populated fields can also include names and DLNs of additional members of the consumer's household.

4. Insurers have their own independent obligations to keep private data secure. In addition, the prefill data contract between the insurer and the third-party data provider imposes a separate duty to safeguard this information.

Respondent Root Exposed New Yorkers' Private Information Through Its Website Tools

5. Respondent Root is a company based in Columbus, Ohio, that engages in the automobile insurance business.

6. As part of this business and at all relevant times, Root maintained a public-facing quoting application on its website, www.joinroot.com. Individuals could use an automated process to request an auto insurance quote from Root by providing limited information about themselves, such as name and address. Root would use this limited information to retrieve

additional relevant information from third party data providers, including the individual's driver's license number ("DLN") and other household members' DLNs.

7. These third-party databases contain vast amounts of personal data, including the private information of New York residents as defined by General Business Law ("GBL") §§ 899-aa and 899-bb, collected from a variety of sources.

8. At the end of the insurance quoting process, Root would provide the user with a pre-filled PDF Application for Insurance. This Application for Insurance included the full, unmasked DLN of the user and their household members, which had been retrieved from the third-party data provider.

9. In late January 2021, threat actors exploited this design failure in Root's quoting tool and used automated scripts to repeatedly request individuals' DLNs from Root. Threat actors were able to acquire more than 44,000 New Yorkers' DLNs in this manner.

10. 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 of these attacks.

Threat Actors Exploited Root's Quote Tool to Access New Yorkers' Private Information.

11. On or around January 19, 2021, threat actors began targeting Root's public website, www.joinroot.com, to access the DLNs of individuals. Threat actors input limited information into the quote tool, causing the prefill function to return private information about the individuals and members of that individual's household. This also generated an Application for Insurance PDF that disclosed these individuals' DLNs.

12. On January 27, 2021, a Senior Manager of Marketing Analytics at Root observed an unusual increase in the number of unattributed profiles being created on joinroot.com. Unattributed profiles have no indicator of how the individual had been directed to Root. The Security Incident team was alerted as this suggested automated robot or “bot” activity was being used to attack the tool in some way. That same day, Root adopted certain attack mitigation measures, including a temporary CAPTCHA that requires humans to solve a puzzle before proceeding. The information security team also took steps to block the automated traffic associated with such attacks.

13. The next day, on January 28, 2021, Root’s information security team realized that the quoting tool that was being attacked exposed individuals’ unmasked DLNs. The incident was then elevated to Root’s Incident Response team, which implemented additional security measures, including temporarily disabling the DLN lookup and prefill functions.

14. By February 2, 2021, Root had permanently masked the DLNs in the quoting flow and Application for Insurance, effectively preventing attackers from continuing to access individuals’ DLNs. Root subsequently adopted several additional measures to deter similar attacks, including implementing a CAPTCHA and monitoring to detect automated attacks.

15. From the time that attackers began to exploit Root’s systems until Root effectively foreclosed the ability to access additional DLNs, attackers were able to access and obtain approximately 72,852 DLNs, of which approximately 44,449 were New York DLNs.

16. The focus on New York DLNs was intentional, as the attack was conducted in large part to conduct unemployment benefits fraud in New York.

Root Did Not Protect Private Information Accessible Through Its Instant Quote Tool.

17. Root failed to adopt reasonable safeguards to protect the private information of New Yorkers that it licensed and transmitted through its computer systems via the quoting tool. This enabled threat actors to harvest tens of thousands of DLNs from Root's systems.

18. Root's risk assessments did not adequately assess the potential risks of handling private information within its public-facing web applications. As a result, Root did not identify this design failure and take steps to protect consumer's private information. Root also did not authenticate a user prior to retrieving and displaying DLNs in plain text on the face of the Application for Insurance.

19. Root also failed to use basic rate limiting tools to prevent repeated use of the instant quote application. Root did not employ adequate mechanisms to deter automated traffic from its instant quote application. Indeed, an internal risk assessment (concluded shortly after the incident at issue) found that Root had, among other things, insufficient controls around automated attacks on and data leakage from its production networks.

20. Root also did not maintain adequate written procedures, guidelines and standards designed to ensure the use of secure development practices for in-house developed applications that it used or otherwise to ensure the confidentiality and security of consumer private information.

Respondent's Conduct Violated New York Law

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

22. GBL § 899-bb requires any person or business that owns or licenses computerized data which includes 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, when unencrypted, an individual's name in

combination with their DLN. GBL §§ 899(bb)(1)(b), 899-aa(1)(b).

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

24. Respondent neither admits nor denies OAG's Findings, paragraphs 1-23 above.

25. OAG finds the relief and agreements contained in this Assurance appropriate and in the public interest. THEREFORE, 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

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

a. "API" means application programming interface.

b. "Biometric Information" means data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual's identity.

c. "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.

d. "Private Information" means (i) information that can be used to identify a natural person in combination with any of the following: Social Security number, any government ID number including driver's license number, financial account number

including debit and credit card numbers, Biometric Information; or (ii) a username in combination with a password or security question and answer that would permit access to an online account.

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

GENERAL COMPLAINT

27. 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

28. Respondent shall maintain a comprehensive information security program (“Information Security 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 the requirements detailed in paragraphs 31- 37 and the following processes:

- a. Assess, update, 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 (as defined in paragraph 31, *infra*);
- 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, 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. Assess, update, 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.

29. Respondent shall 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 but not be limited to the following: the staffing and budgetary sufficiency of the Information Security Program, the degree to which the Information Security Program has been implemented, challenges to the success of the Information Security Program, the existing and emerging security risks faced by Respondent, and any barriers to the success of the Information Security Program.

30. 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 and shall implement appropriate training of such employees. The notice and training required under this paragraph shall be provided to the appropriate employees within ninety (90) days of the Effective Date of this Assurance, or within forty-five (45) days of when an employee first assumes new responsibility for implementing, maintaining, assessing, updating, or monitoring the Information Security Program. Respondent shall document that it has provided the notices and training required in this paragraph.

SPECIFIC INFORMATION SECURITY REQUIREMENTS

31. Data Inventory: Within ninety (90) days of the Effective Date of this Assurance, to the extent it has not already done so, Respondent shall develop and maintain a data inventory of all instances in which it collects, uses, stores, retrieves, transmits, displays, maintains and/or otherwise processes Private Information. Respondent shall update and document its data inventory not less than annually. The data inventory shall, at a minimum, include the processes listed below. Root may, in the performance of the first Data Inventory required by this paragraph, discover that it is not in compliance with the terms of this Assurance. In such circumstances, Root will be considered in compliance with the terms of this Assurance so long as

Root resolves the issue in a reasonable time period (not to exceed 60 days from discovery of the issue). Nothing in this paragraph relieves Root from any legal, regulatory, or contractual obligation it otherwise has in relation to its information security program including, but not limited to, responding to and reporting any additional data breaches.

a. Identify all points at which Private Information is collected, used, stored, retrieved, transmitted, displayed, maintained, or otherwise processed;

b. Map and/or track the complete path of all data flows involving Private Information, including API calls; 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.

32. 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.

33. Secure Software Development Lifecycle: Beginning within ninety (90) days of the Effective Date of this Assurance, Respondent shall maintain written policies and procedures designed to ensure secure software development practices for and regular security assessments and testing of all web-based, mobile, or other applications—whether public-facing, credential-based, or internal—maintained by or on behalf of Respondent that collects, uses, stores, retrieves, transmits, displays, maintains and/or otherwise processes Private Information. To the extent that a third-party is providing the application, Root shall take reasonable steps to implement this requirement which may vary depending on the source of the application. Such

policies and procedures must include the following requirements:

- a. Wherever Private Information is implicated by the regular and expected use of any such application, Respondent shall consider the privacy impact at each relevant stage of the software development lifecycle process;
- b. Wherever Private Information is implicated by the regular and expected use of any such application, Respondent shall include reasonably designed privacy testing and documented approval each time the application is changed or updated;
- c. 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;
- d. For external software development vendors, evaluate, assess, and test adherence to Respondent's secure development procedures, guidelines, and standards or reasonably equivalent secure development standards.

34. Authentication: Respondent shall maintain reasonable account management and authentication procedures, including the use of MFA (or a reasonably equivalent control), for access to unredacted Private Information or remote access to Respondent's Network; provided that until December 31, 2025 Root will be considered in compliance with the terms of this paragraph so long as a customer account (a) is secured by mandatory MFA (or a reasonably equivalent control) or (b) does not provide access to any unredacted Private Information and (no later than October 16, 2024) is secured by optional MFA (or a reasonably equivalent control). For the avoidance of doubt, it shall not violate this section of the Assurance for Respondent to provide a non-account based, non-MFA, public-facing consumer tool (e.g., new insurance coverage quotes) that does not disclose any unredacted Private Information.

35. Web Application Defenses: Respondent shall maintain reasonable safeguards to prevent Security Events through attacks on web applications. Such safeguards shall at least include the use of appropriate bot detection and mitigation tools.

36. Monitoring: Beginning within ninety (90) days of the Effective Date of this Assurance, Respondents shall maintain systems designed to collect and monitor Network activity, as well as activity on any platforms or applications operated by or on behalf of Respondent, that collect, use, store, retrieve, transmit, display, maintain, or otherwise process Private Information. Respondent shall also establish and maintain reasonable policies and procedures designed to properly configure such tools to report anomalous activity. The systems shall, at a minimum: (i) provide for centralized logging and monitoring that includes collection and aggregation of logging for Respondent's Network and any platforms or applications operated by or on behalf of Respondent that collect, use, store, retrieve, transmit, display, maintain, or otherwise process Private Information, and (ii) monitor for and alert security personnel to suspicious activity. Activity logs should be immediately accessible for a period of at least 90 days and stored for at least one year from the date the activity was logged.

37. Threat Response: Whenever Respondent is aware of or reasonably should be aware of a reasonable risk of a Security Event, Respondent shall:

a. Promptly investigate and monitor for suspicious activity any platforms or applications operated by or on behalf of Respondent and any places on its Network that collect, use, store, retrieve, transmit, display, or maintain, or otherwise process Private Information; monitoring shall be at a level that is sufficiently granular to detect a potential Security Event;

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.

38. For the avoidance of doubt, to the extent that Root contracts with any third party to provide services subject to the provisions of this Assurance, Root shall take reasonable steps to ensure that the material terms of this Assurance are satisfied.

OAG ACCESS TO RECORDS

39. Respondent shall retain any documentation and reports required by paragraphs 28-37 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. No documents may be withheld on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney-client privilege, statutory exemption, or any other claim.

MONETARY RELIEF

40. Respondent shall pay to the State of New York \$975,000.00 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 AOD No. 25-009.

MISCELLANEOUS

41. 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 48, 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 to such action or proceeding based upon personal jurisdiction, inconvenient forum, or venue. Root does not concede that it is subject to New York jurisdiction other than with respect to the terms of this Assurance;
- 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).

42. 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.

43. This Assurance is not intended for use by any third party in any other proceeding.

44. 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.

45. 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.

46. 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.

47. All notices, reports, requests, and other communications pursuant to this Assurance must reference Assurance No. 25-009, 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:

Jodi Baker, or in her absence, to the person holding the title of

General Counsel
Root, Inc.
80 E. Rich St, Ste 500
Columbus, OH 43215
Jodi.baker@root.com

If to the OAG, to the person holding the title of Bureau Chief, Bureau of Internet & Technology.

48. 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 1-25 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.

49. 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.

50. 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 Root Insurance Company, by Jodi Baker, as the signatory to this AOD, is a duly authorized officer acting at the direction of the Board of Directors of Root Insurance Company.

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

52. 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.

53. 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.

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

55. 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.

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


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

58. 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.

59. 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.

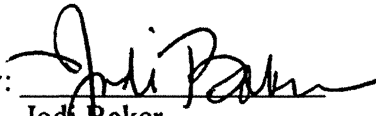
60. The effective date of this Assurance shall be the date the OAG signs this Assurance.

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: 3/20/25

ROOT INSURANCE COMPANY

By: 
Jodi Baker
Vice President, General Counsel &
Secretary
Root, Inc.
80 E. Rich St, Ste 500
Columbus, OH 43215

Date: March 5, 2025