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

In the Matter of

Assurance No. 25-045

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

HARTFORD FIRE 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 reported by Hartford Fire Insurance Company ("The Hartford" or "Respondent"). This Assurance of Discontinuance ("Assurance") contains the findings of OAG's investigation and the relief agreed to by the OAG and The Hartford (collectively, the "Parties"), whether The Hartford 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 to generate insurance quotes. These quoting tools are designed with a data "prefill" capability to obtain additional information about the individual from third party databases. When a user enters basic personal details—such as name, date of birth, and/or address—a quote tool with prefill capabilities will obtain additional private information about the person from such databases. Quoting tools for consumers are available on the public websites of many insurance

companies.

2. To provide prefill functionality, insurance companies contract with third-party data providers to license the use of the data providers' information. The data providers' databases contain 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 a quoting tool with prefill capability, the tool transmits the information to the prefill 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 insurance company. The insurance company's tool then uses the data to generate an insurance quote and displays the quote to the individual using the tool.

3. The purpose of prefilling this data is to automatically obtain information necessary for an auto quote that the average consumer might not know from memory, such as the consumer's driver's license number ("DLN") or vehicle identification number. In addition, where prefill is used, it often provides the auto insurance company with the names, dates of birth, and DLNs of additional members of the person's household.

Threat Actors Obtained New Yorkers' Private Information Through The Hartford's Quoting Tools

4. Respondent The Hartford is a company headquartered in Hartford, Connecticut, that engages in the automobile insurance business. It is licensed to sell insurance products to consumers in New York.

5. As part of this business, and at all relevant times, The Hartford maintained a public-facing quoting application on its website, www.thehartford.com, (the "Consumer Tool"), and an insurance agent quoting tool on a password-protected website (the "Agent Tool").

6. When a person's name and birthdate or address were entered into The Hartford's Consumer Tool, The Hartford used a third party data provider to prefill that person's DLN and the names, DLNs, birthdates of other drivers in their household. The Consumer Tool displayed to the user a "masked" or partially redacted version of the person's DLN and the DLN of the other drivers in their household. The "source data" of the Consumer Tool website, however, contained a complete version of this private information. This unredacted consumer information in the website's source data could be accessed using the internet browser's built-in website developer tools.

7. The Hartford Agent Tool was accessible on a website that required agent credentials to access it -- i.e., a password and username. The Agent Tool website did not, during the relevant time, require users to verify their identity with multifactor authentication. After the agent credentials had been entered, the Agent Tool could generate an auto quote in a similar manner to the Consumer Tool. Once the user entered the basic information for an individual, the Agent Tool displayed the individual's personal information including their DLN, and the name, DLN and birthdate of the other drivers in their household. Although the Agent Tool displayed the full driver's license number to agents, those agents did not require this information to perform their quoting related tasks.

8. From early December 2020 through March 2021, threat actors repeatedly exploited the errors in the implementation of The Hartford's Consumer Tool and Agent Tool. Threat actors were able to access over 32,000 New Yorkers' DLNs in this manner.

The Attacks on The Hartford's Auto Quoting Tools.

9. In December 2020, threat actors began targeting The Hartford's Consumer Tool on its public website, www.thehartford.com. Threat actors input certain information about an individual into the quote tool, causing the prefill function to return private information about the

individual and members of that individual's household. The DLNs associated with those individuals were visible in the website's source data using website developer tools built into the internet browser of website visitors.

10. On January 11, 2021, a business unit at The Hartford observed an increase in the number of consumer auto quote requests and began investigating. The Hartford's enterprise level information security team was alerted to the issue on January 19, 2021 and began its own investigation. DLNs were removed from the Consumer Tool website data on January 29, 2021. Dates of birth were removed from the Consumer Tool website data on February 2, 2021. The attack on the Consumer Tool was terminated by The Hartford on February 3, 2021 after The Hartford implemented measures to deter such attacks.

11. On February 7, 2021, threat actors began attacking The Hartford's Agent Tool. This attack was discovered by The Hartford's information security team on March 3, 2021. This attack was terminated by The Hartford on March 4, 2021 after The Hartford implemented measures to deter such attacks.

12. From the time that attackers began to exploit The Hartford's systems until The Hartford effectively foreclosed the ability to access additional DLNs, attackers were able to access and obtain over 32,000 New York DLNs.

13. Many of the New York DLNs that were 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.

The Hartford Did Not Adequately Protect Private Information Accessible Through Its On-line Quote Tools.

14. The Hartford did not adequately protect the private information of New Yorkers that was transmitted from third-party providers to the quoting tools.

15. The Hartford maintains it had reasonable information security policies in place to protect consumer data utilized by the quoting tools that were attacked, including policies regarding access control and application development. While this may be the case, some of the policies were not implemented effectively which, at the time of the incident, impacted The Hartford's ability to prevent, detect, and/or respond to the attack. For example:

a. The Hartford conducted frequent "penetration tests" of its systems that it maintains were designed, reviewed by outside consultants, and executed to detect certain important security issues. While this may be the case, those penetration tests were not designed to detect the specific design errors exploited by the threat actors. As a result, The Hartford's penetration tests did not identify and The Hartford did not immediately address the specific design errors that were exploited in the attacks.

b. At the time of the attacks in 2021, The Hartford also had not updated the fraud prevention and abuse detection procedures for its auto quotation tools, which allowed the attacks to go undetected for the time period discussed above.

c. The Hartford's Agent Tool site was password protected, but the password protocol it required users to follow was out of date and the system did not at that time use multifactor authentication to confirm user identity.

Respondent's Violations

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

17. 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). GBL §§ 899(bb)(1)(b), 899-aa(1)(b).

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

19. Respondent neither admits nor denies the OAG's Findings, in paragraphs 1-18 above.

20. 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

24. 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 other equipment or services (i) that are capable of using, exchanging, or sharing software, data, hardware, or other resources, (ii) that 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

25. 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

26. Respondent shall, to the extent it has not already done so, 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. 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 29-35 and the following processes:

a. Evaluate, 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 Access Assessment;

b. Design, implement, and maintain reasonable administrative, technical, and physical safeguards to manage 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 26(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 26(b) above.

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 a material impact on the effectiveness of the Program, and document any adjustments; and

f. 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.

27. Respondent shall, to the extent it has not already done so, designate a qualified employee responsible for implementing, maintaining, evaluating, updating, and monitoring the Information Security Program. The designated employee shall have the experience 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"). 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 twice a year to Respondent's Chief Executive Officer (or the equivalent thereof) and at least 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 sufficiency of resources allocated to the Information Security Program, the overall effectiveness of the Information Security Program, and any material cybersecurity risks.

28. 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 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 responsibilities for implementing, maintaining, evaluating, updating, or monitoring the Information Security Program, whichever is later. Respondent shall document that it has provided the notices and training required in this paragraph.

Specific Information Security Requirements

29. Data Access Assessment: Within one hundred eighty (180) days of the Effective Date of this Assurance, Respondent shall, to the extent it has not already done so, review all instances in which it provides access to Private Information, consider mitigating controls in a risk assessment, and reasonably ensure that access is limited to the minimum level necessary to

accomplish a defined task. Respondent shall review, update, and document its provision of access to Private Information not less than annually.

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

31. Secure Software Development Lifecycle: Respondent shall, to the extent it has not already done so, maintain written policies and procedures designed to reasonably 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 requirements:

a. 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 process, 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;

32. For external software development vendors, comply with Paragraph 26(f) of this Assurance.

33. Authentication: Respondent shall maintain reasonable account management and authentication procedures, including the use of multifactor authentication (or a reasonably equivalent control) for access to Respondent's information systems that provide access to Private Information or remote access to Respondent's Network.

34. Monitoring: Respondent shall, to the extent it has not already done so, maintain a system reasonably designed to collect and monitor Network activity (including with respect to third-party service providers, complying with paragraph 26(f) above), 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 any platforms or applications operated by or on behalf of Respondent that collect, maintain, use, or disclose Private Information, and (ii) monitor for suspicious activity and alert security personnel. 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.

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

a. Promptly monitor for indicators of suspicious activity (or with respect to a third-party service provider, complying with paragraph 26(f) above) and 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

36. Respondent shall retain the documentation and reports required by paragraphs 26-35 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 would otherwise be protected as attorney work product or under the attorney-client privilege.

MONETARY RELIEF

37. Respondent shall pay to the State of New York eight hundred and fifteen thousand dollars ($815,000). Payment shall be made in full within ten (10) business days of the Effective Date of this Assurance. Payment shall be made by wire transfer in accordance with instructions provided by an OAG representative and shall reference AOD No. 25-045.

MISCELLANEOUS

38. 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 46, 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).

39. 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.

40. 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.

41. 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.

42. 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.

43. Nothing contained herein shall be construed as to deprive any person of any private right under the law.

44. 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.

45. All notices, reports, requests, and other communications pursuant to this Assurance must reference Assurance No. 25-045, 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: the person holding the title of General Counsel.

Hartford Fire Insurance Company
Office of General Counsel
690 Asylum Avenue
Hartford, CT 06155

If to the OAG, to:

Bureau Chief
Bureau of Internet & Technology
Office of the Attorney General of New York State
28 Liberty Street
New York, NY 10005.

46. 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 the OAG's Findings, paragraphs 1-18 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.

47. 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.

48. 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 The Hartford, by Donald C. Hunt, as the signatory to this AOD, is a duly authorized officer acting with the knowledge of the Board of Directors of The Hartford.

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

50. 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.

51. 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.

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

53. 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.

54. Respondent acknowledges that it has entered this Assurance freely and voluntarily and upon due deliberation with the advice of counsel.

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

56. 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.

57. 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.

58. 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
Gena Feist
Assistant Attorney General
Bureau of Internet & Technology
28 Liberty Street
New York, NY 10005

Date: 10/8/25

HARTFORD FIRE
INSURANCE COMPANY

By: ______________________
Donald C. Hunt
Executive Vice President and General Counsel
Hartford Fire Insurance Company
Office of General Counsel
690 Asylum Avenue
Hartford, CT 06155

Date: October 2, 2025