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

In the Matter of

Assurance No. 25-044

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

Hagerty Insurance Agency,

Respondent.

ASSURANCE OF DISCONTINUANCE

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

FINDINGS OF THE OAG

1. Many automobile insurance companies provide a website to generate insurance quotes. These insurance 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—an insurance quote tool with prefill capabilities will populate other fields with additional private information about the person. Similar quoting tools for insurance agents are also made available through the internet, often through a special internet website for insurance agents.

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, birthdates, and DLNs of additional members of the consumer's household.

4. The data in automatically populated fields does not need to be displayed to the public in order to be utilized by the insurer to generate the automobile insurance quote. 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 Did Not Adequately Protect Private Information Accessible Through Its Website Tools.

5. Respondent Hagerty Insurance Agency is an insurance company based in Michigan. Hagerty is licensed to sell insurance products to consumers in New York state.

6. As part of this business and at all relevant times Hagerty maintained public-facing auto insurance quoting applications on the internet, including two consumer facing auto insurance quote tools (collectively the "Consumer Quoting Tools") and a password protected internet website for insurance agents that allowed them to access an auto insurance quote tool (the "Agent Quoting Tool").

7. Users of the Consumer Quoting Tools could access an automated process to request an auto insurance quote from Hagerty by providing limited information about an individual, such as name and address. Hagerty would use this limited information to retrieve additional relevant information from third party data providers, including the individual's DLN and birthday, as well as birthdates and DLNs of other members of the household.

8. The Agent Quoting Tool required an agent's login credentials to sign in. Users had the ability to self-create broker accounts, which were subject to Hagerty approval for full user rights. Simply creating such an account, however, gave those users access to the Agent Quoting Tool. Once logged in, visitors could use an auto insurance quoting tool by inputting an individual's name, address, and/or date of birth in order to retrieve that person's private information. The retrieved data included the same private information noted in the paragraph above.

9. While the private information of the individual and members of their household was necessary for Hagerty's system to generate an insurance quote, it was **not** necessary for users of the Consumer Quoting Tools or Agent Quoting Tool to have access to this information. These tools were also not protected by standard threat detection tools.

10. The Agent Quoting Tool exposed the full, plain text DLNs and dates of birth on the face of the tool. Additionally, while the DLNs and dates of birth displayed on the face of the Consumer Quoting Tools were partially redacted, this private information was displayed in plain text in the html source code.

Threat Actors Exploited Respondent's Consumer Quoting Tools and Agent Quoting Tool to Access the Private Information of New York Residents.

11. On January 31, 2021, threat actors began exploiting the coding error on Respondent's primary Consumer Quoting Tool. Respondent's website team failed to immediately identify the threat. While the team noticed a spike in abandoned quotes, they did not realize that private information was accessible in the website source data. They initially believed this was an attempt to gather information about their quoting process and took steps to slow the use of bots.

12. On February 16, 2021, Respondent received a fraud alert from the NYS Department of Financial Services regarding attacks on auto insurance websites designed to harvest DLNs. Respondent's information security team conducted a review of the activity on the primary Consumer Quoting Tool website and discovered that DLNs and dates of birth were visible in the source code. Respondent's information security team turned off the instant quote feature the same day.

13. On February 23, 2021, Respondent relaunched the primary Consumer Quoting Tool after ensuring that DLNs and dates of birth were not accessible in the source code.

14. On March 1, 2021, Respondent's monitoring system noticed another spike instant quoting activity and Respondent tracked it to a "legacy" Consumer Quoting Tool that Respondent IT staff did not realize was operational. The legacy Consumer Quoting Tool website also exposed DLNs and birthdates in its source code. Respondent took steps to shut down the

legacy Consumer Quoting Tool the same day.

15. On or around February 16, 2021, Respondent discovered that threat actors had also been exploiting the weak account creation requirements of the Agent Quoting Tool website to access it without authorization. The Agent Quoting Tool prefill function returned personal and private information about a consumer and drivers in their household. This information appears in plain text on the website as well as in the source code. Respondent shut down the prefill function the same day the attack was discovered and relaunched it after strengthening security for the agent website and Agent Quoting Tool.

16. 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.

17. Respondent has implemented certain measures to prevent future attacks.

18. On April 13, 2021, Respondent started notifying affected New York state residents of the breach. Respondent also offered impacted consumers one-year of complementary identity monitoring services.

Respondent Did Not Protect Private Information Accessible Through Its Website Tools.

19. Respondent failed to adopt reasonable safeguards to protect the private information of New Yorkers that it licensed and transmitted through its computer systems. This enabled threat actors to harvest approximately 66,000 DLNs and birthdates of New Yorkers from Respondent’s systems.

20. Two of the three quoting tools were developed internally by Respondent – the primary Consumer Quoting Tool and the Agent Quoting Tool. These tools had design errors that should have been detected by Respondent during development and after deployment.

21. The legacy Consumer Quoting Tool was developed by a company Respondent had acquired. Although the website used private information that was protected by law, at the time of the attack Respondent's information security team was not actively monitoring and protecting the legacy website, believing it to have been decommissioned.

22. Prior to the attacks, none of the three tools had been subject to a specific privacy impact assessment by Respondent. These websites, however, were protected by standard security controls, such as IP blocking, rate limiting, rate monitoring, CAPTCHA, or website application firewalls, and Respondent did conduct various privacy assessments related to its overall systems.

23. Respondent's Agent Quote Tool did not authenticate new users, did not require multifactor authentication, and did not have adequate attack prevention and detection measures in place.

24. Respondent's primary Consumer Quoting Tool and Agent Quote Tool exposed sensitive personal information in the Agent Quote Tool without there being any need for users or insurance agents to view it.

25. As a result, threat actors were able to harvest approximately 66,000 New Yorker DLNs and birthdates from Respondent's systems. A subset of the DLNs and birthdates were then used to submit fraudulent unemployment claims with the New York State Department of Labor.

Respondent's Conduct Violated New York Law

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

27. 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).

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

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

30. 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

31. 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 COMPLAINCE

32. 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

33. 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 36-42 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.

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.

34. 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.

35. 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 sixty (60) days of the Effective Date of this Assurance, or within thirty (30) 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

36. Data Inventory: Within sixty (60) 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.

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.

37. 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, including, but not limited to, prefill data providers.

38. Secure Software Development Lifecycle: 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, Respondent 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.

39. Authentication: Respondent shall maintain reasonable account management and authentication procedures, including the use of multifactor authentication ("MFA") (or a reasonably equivalent control), for access to unredacted Private Information or remote access to Respondent's Network.

40. 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.

41. Monitoring: Respondents shall maintain reasonable 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.

42. 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.

OAG ACCESS TO RECORDS

43. Respondent shall retain any documentation and reports required by paragraphs 32-42 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

44. Respondent shall pay to the State of New York $1,300,000 in penalties, fee, and costs. Payment 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. 25-044.

MISCELLANEOUS

45. 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 52, 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. Respondent 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).

46. 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.

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

48. 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.

49. 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.

50. 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.

51. All notices, reports, requests, and other communications pursuant to this Assurance must reference Assurance No. 25-044, 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:

Diana Chafey, or in her absence, to the person holding the title of Chief Legal Officer

Chief Legal Officer
Hagerty Insurance Agency
121 Drivers Edge
Traverse City, MI 49684
dchafey@hagerty.com

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

Bureau Chief
Bureau of Internet & Technology
28 Liberty Street
New York, NY 10005

52. 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 1-28 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.

53. 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.

54. 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 Hagerty Insurance Agency, by Chief Legal Officer Diana Chafey, as the signatory to this AOD, is a duly authorized officer acting at the direction of the Board of Directors of Hagerty Insurance Agency.

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

56. 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.

57. 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.

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

59. 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.

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

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

62. 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.

63. 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.

64. 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
Gena Feist
Assistant Attorney General
Bureau of Internet & Technology
28 Liberty Street
New York, NY 10005

Date: 10/8/25

HAGERTY INSURANCE AGENCY

By: Diana M Chafey
Diana Chafey
Chief Legal Officer
Hagerty Insurance Agency
121 Drivers Edge
Traverse City, MI 49684

Date: September 22, 2025