

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

In the Matter of

Assurance No. 25-048

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

**AMERICAN FAMILY MUTUAL
INSURANCE COMPANY, S.I.,**

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 American Family Mutual Insurance Company, S.I. (“AmFam” or “Respondent”). This Assurance of Discontinuance (“Assurance”) contains the findings of OAG’s investigation and the relief agreed to by the OAG and AmFam 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 previously saved information and 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. Some companies also check their own internal database for additional information on the individual before querying a data provider.

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 prefill 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. The data in automatically populated fields does **not** need to be displayed in full to the user in order to be confirmed by the user or utilized by the insurer to generate the automobile insurance quote.

5. Insurers have their own independent obligations to keep private data secure.

Respondent Did Not Adequately Protect Private Information Accessible Through Its Instant Auto Insurance Quote Tools.

6. Respondent AmFam is a company headquartered in Wisconsin that engages in the automobile insurance business. AmFam's subsidiary, Midvale Indemnity Company, is licensed to sell insurance products to consumers in New York State.

7. As part of this business, at all relevant times Respondent maintained multiple publicly accessible instant auto insurance quote website applications for consumers. When a person's name and birthdate or address were entered into these tools, AmFam used previously saved information and/or a third party data provider to prefill that person's DLN and birthdate, and the names, DLNs, birthdates of other drivers in their household.

8. AmFam exposed the private information of consumers in the source data of these websites, which was easily viewable with the developers' tools built into every web browser. Six of these tools displayed to the user the full, unredacted DLN and birthdate associated with the name and the DLN of the other drivers in their household in the source data of the website (collectively the "Consumer Tools"). During the course of the attacks, AmFam received multiple industry advisories regarding a widespread campaign to steal DLNs from auto insurance quoting tools. These advisories included specific warnings regarding using browser developer tools to view DLNs exposed in the website source data

9. Two of the Consumer Tools exposed full DLNs in the source data of the website after December 13, 2020, when a data protector service or "DPS" that protected private information was retired from use by AmFam (the "Short Term Exposure Tools").

10. Four of the Consumer Tools exposed full DLNs for longer periods, in some cases months and in one case up to five years prior to the attacks (the "Long Term Exposure Tools").

11. Regarding the Long Term Exposure Tools, prior to the attacks AmFam had not conducted a private information inventory that tracked them. As a result, AmFam was not reasonably able to ensure that such private information was protected.

12. Regarding the Short Term Exposure Tools, during the 2020 DPS retirement process AmFam failed to reasonably identify, test, and protect the Short Term Exposure Tools.

AmFam:

- a) did not create an inventory of all end user applications using the DPS to protect private information that included the Short Term Exposure Tools;
- b) did not adopt a transition plan that specifically considered the Short Term Exposure Tools; and
- c) did not perform a risk assessment specific to the Short Term Exposure Tools.

13. As a result, AmFam was not reasonably able to ensure that the private information utilized by the Short Term Exposure Tools and the Long Term Exposure Tools would be protected after the DPS retirement and could not reasonably confirm that this previously protected private information remained secure.

14. From January 2021 through March 2021, and again in December 2021, threat actors repeatedly exploited AmFam's information security errors to exploit the Short Term Exposure Tools and the Long Term Exposure Tools. These attacks exposed the DLNs of approximately 200,000 New Yorkers.

15. 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").

The Attacks on Costco Choice, OnStar Choice, and the Midvale Auto Quote Tools

16. Costco Choice (www.CostcoChoice.com) and OnStar Choice (www.Onstarinsurance.com) were launched in early 2020 and began utilizing prefill in August 2020. These auto quote tools exposed plaintext prefilled DLNs in the source data of the website. Although the websites that hosted the Choice tools were the subject of multiple general website security tests, those tests were not designed to check for the plain text exposure of private

information in the source data.

17. The Midvale Auto Quote Tool (go.midvaleinsurance.com) was launched in 2017. Prior to December 2020, this auto insurance quoting tool was protected by a DPS that redacted private data such as DLNs and dates of birth. This DPS tool was retired in December 2020. Although the Midvale Auto Quote Tool was tested during the DPS retirement process, that testing was not reasonably designed to identify the exposure of private information in the source data of the website. As a result, the Midvale Auto Quote Tool exposed private information on the face of the website for approximately a month prior to the January 2021 attack.

18. Within days of the DPS retirement, AmFam's information technology team realized that the DPS retirement had "broken" some functions of the Midvale Auto Quote Tool. While the tool was fixed and re-tested, once again this testing failed to identify the exposure of private information in the source data of the website.

19. The DPS was retired on December, 13, 2020. The first three attacks started January 19, 2021 and AmFam's information technology team turned off consumer data prefill by January 28, 2021.

20. The driver's license numbers of over 97,000 New Yorkers were exposed in the first three attacks.

The Attack on the American Family Auto Quote Tool

21. The American Family Auto Quote Tool (www.Autoquote.amfam.com) was launched at least as early as 2011. Like the Midvale Insurance Auto Quoting Tool, prior to December 13, 2020, this auto insurance quoting tool was protected by a DPS that redacted or "masked" private data such as DLNs. This tool became unprotected when the DPS was retired in December 2020.

22. Although testing was performed related to the retirement of the DPS and the new security solution, the American Family Auto Quote Tool was not subject to reasonable testing in relation to the DPS retirement.

23. The American Family Auto Quote Tool attack started February 6, 2021, a week after the first three attacks were terminated. This attack was not detected for another six weeks. On March 18, 2021, AmFam's prefill provider, who was aware of the industry-wide attacks on auto-insurance prefill, alerted AmFam to an excessive number of requests that suggested an attack was taking place. This attack was terminated on March 19, 2021.

24. The driver's license numbers of approximately 100,000 New Yorkers were exposed in this attack.

The Midvale Bound Policy Attack and American Family / Homesite Life Direct Attack

25. The Midvale Bound Policy Attack involved a manual process with more steps than the first four attacks. This attack involved the threat actor purchasing a policy with invalid financial credentials and then either (a) printing a PDF copy of the new policy after purchase or (b) accessing the target individual's DLN in the newly created user account. These features were added least as early as 2016 and allowed threat actors taking the steps described above to access private information from their launch date. This tool was not tested for private data exposure by AmFam information security prior to the attacks.

26. The Midvale Bound Policy Attack started on January 28, 2021 and was terminated on March 26, 2021. This attack was terminated when AmFam adopted new security policies in response to the attacks on the Costco Choice Tool, OnStar Choice Tool, Midvale Auto Quote Tool, and American Family Auto Quote Tool.

27. The American Family / Homesite Life Direct Attack was similar to the first four

attacks. It involved plain text data exposure on the face of a public website that used prefill. This feature was launched in 2015 but was not tested for private information exposure by AmFam information security prior to the attacks.

28. The American Family / Homesite Life Direct Attack started on December 5, 2021, was detected on December 10, 2021, and was terminated on December 11, 2021.

29. The driver's license numbers of approximately 350 New Yorkers were exposed in these three attacks.

AmFam Did Not Reasonably Protect Private Information Accessible Through Its Consumer Tools.

30. AmFam failed to adopt reasonable safeguards to protect the private information of New Yorkers that it licensed and transmitted through its computer systems via the Consumer Tools. This enabled threat actors to harvest approximately two hundred thousand New Yorker DLNs from AmFam's systems.

31. Respondent did not conduct private information data inventories that included the attacked auto quoting tools, which would have assisted it in preventing or responding to attacks. As a result, Respondent suffered multiple attacks over the course of a year.

32. Respondent's security program did not assess the potential risks of handling private, nonpublic, or otherwise sensitive consumer information within the attacked auto quoting tools.

33. Respondent's security testing was not designed to discover plain text DLNs in the website source data.

34. Respondent also did not maintain adequate processes to ensure the confidentiality and security of private information accessed through the prefill process.

35. Respondent's Consumer Tools did not reasonably protect private information,

including prefilling in plain text full DLNs of a query subject and household members (i) in the source data of the website and (ii) in a fraudulently created new member account even when the method of payment was invalid.

36. Respondent did not employ reasonable technological means to detect, prevent, or respond to an attack, for example:

- a) AmFam did not implement automated baseline tracking of user traffic to the attacked tools or monitor ongoing traffic to detect unusual activity that would indicate an attack. As a result, AmFam failed to immediately discover the attacks on its Consumer Tools by the exponential increase in use. Indeed, a post attack analysis showed that during the attack some AmFam tools received up to fifteen times the user quotation requests that they received pre-attack. Similarly, during the attacks AmFam received up to five times the daily prefill requests it had received prior to the attacks.
- b) AmFam did not adopt geographic filtering tools to block or review all auto insurance requests for United States insurance that originated outside the United States.
- c) AmFam did not block prefill for individuals who did not live in locations where AmFam did not write insurance.
- d) AmFam did not use reCAPTCHA to confirm Consumer Tools users were human.
- e) AmFam did not track how many times a particular IP address was used to request a quote to limit or block IPs seeking repeated quotes, which can indicate an attack.

- f) AmFam did not require addresses entered with an individual's name to match their actual address or otherwise track entered addresses to detect fraud.

37. After the first three tools were attacked, Respondent's security team failed to identify similar vulnerabilities in the other tools. In the case of the American Family / Homesite Life Direct Attack, this attack started almost a year after the first three attacks were terminated.

38. Finally, in retiring the DPS that protected a wide range of private information, Respondent did not create an inventory of all tools using DPS protected data, did not reasonably test all tools using DPS protected data prior to DPS retirement, and did not reasonably review all such tools after the DPS retirement.

Respondent's Conduct Violated New York Law

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

40. 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).

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

42. Respondent neither admits nor denies OAG's Findings, paragraphs 1-41 above.

43. 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

44. 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 protected by Executive Law § 63(12) or GBL § 899-bb 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 COMPLIANCE

45. 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

46. 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 referred to in the first sentence of this subsection shall, at a minimum, include all the requirements detailed in paragraphs 49-56 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.

47. 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.

48. 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

49. 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.

50. 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.

51. 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, AmFam shall take reasonable steps to implement this requirement which may vary depending in the source of the application. Such policies and procedures must include the following requirements:

d. 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;

e. 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;

f. 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;

g. 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.

52. Authentication: Respondent shall maintain reasonable account management and authentication procedures, including the use of multifactor authentication (or a reasonably

equivalent control), for access to unredacted Private Information or remote access to Respondent's Network.

53. 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.

54. 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. To the extent practicable, 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.

55. 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.

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

OAG ACCESS TO RECORDS

57. Respondent shall retain any documentation and reports required by paragraphs 45-56 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

58. Respondent shall pay to the State of New York two million eight hundred thousand dollars (\$2,800,000) 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 AOD No. 25-048.

MISCELLANEOUS

59. 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 66, 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. AmFam 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).

60. 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.

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

62. 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.

63. 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.

64. 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.

65. All notices, reports, requests, and other communications pursuant to this Assurance must reference Assurance No. 25-048, 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:

Thomas R. Hrdlick, or in their absence, to the person holding the title of

General Counsel
American Family Mutual Insurance Company, S.I.
6000 American Parkway
Madison, WI 53783

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

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

66. 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 1-41 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.

67. 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.

68. 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 American Family Mutual Insurance Company, S.I., by [xxx NAME], as the signatory to this AOD, is a duly authorized officer acting at the direction of the Board of Directors of American Family Mutual Insurance Company, S.I.

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

70. 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.

71. 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.

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

73. 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.

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

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

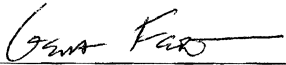
76. The Assurance and all its terms shall be construed as if mutually drafted with no presumption of any type against any party that may be found to have been the drafter.

77. 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.

78. 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
Office of the Attorney General
28 Liberty Street
New York, NY 10005

Date: 10/8/25

American Family Mutual Insurance
Company, S.I.

By: 
Thomas R. Hrdlick
Chief Legal Officer
6000 American Parkway
Madison, WI 53783

Date: 10/8/25