

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

In the Matter of

Assurance No. 25-042

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

Metromile LLC

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 Metromile LLC (“Metromile” or “Respondent”). This Assurance of Discontinuance (“Assurance”) contains the findings of OAG’s investigation and the relief agreed to by the OAG and Metromile whether acting through its respective directors, officers, employees, representatives, agents, affiliates, or subsidiaries (collectively, the “Parties”).

FINDINGS OF OAG

1. Many automobile insurance companies provide a website for use by consumers to generate insurance quotes. These quoting tools are designed with a data “prefill” capability to pull in additional information about the individual from third party databases. When a user enters certain personal details—such as name, date of birth, and/or address—a quoting 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 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 quoting tool, the website application transmits a request to the data provider. The data provider, in turn, identifies the individual associated with those data points, and then returns additional data about the individual to the insurer’s quote tool.

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 also frequently include the names, DLNs, and other personal information of additional members of the 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.

Respondent Metromile Did Not Adequately Protect Private Information Accessible Through Its Insurance Quote Tools

5. Respondent Metromile LLC is an insurance company organized under the laws of the State of Delaware.

6. As part of this business, at all relevant times, Metromile maintained on its website a public-facing instant auto insurance quoting application (the “Auto Quote Tool”). Individuals could use an automated process to request an auto insurance quote from Metromile by providing limited information about themselves, such as name and address. Metromile would use this limited information to retrieve additional relevant information from third party data providers, including the individual’s driver’s license number (“DLN”) and other household members’

DLNs.

7. Metromile exposed the prefilled personal information of consumers in plain text in four ways. First, Metromile exposed the personal information of individuals on the face of the Auto Quote Tool, including date of birth, DLN, and other drivers in the household. Second, Metromile exposed this personal information in the source code of the Auto Quote Tool webpage, which was viewable with the developers' tools built into every web browser. Third, Metromile exposed this personal information on the policy application documents generated at the end of a quote request. Fourth, Metromile exposed this personal information in the online customer account dashboard created upon policy purchase with fraudulent payment information.

8. On December 1, 2020, threat actors began exploiting these design failures in Metromile's Auto Quote Tool and used automated scripts to repeatedly request individuals' DLNs from Metromile. Metromile's implementation of the prefill tool did not require the date of birth or address information entered to be accurate, the individual's DLN and other private information would be prefilled. Over the course of two months, threat actors were able to acquire approximately 90,000 New Yorkers' DLNs in this manner.

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

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

10. On December 1, 2020, threat actors began targeting Metromile's public website, www.metromile.com, to obtain DLNs through its Auto Quote Tool.

11. Threat actors input limited information into the Auto Quote Tool, causing the prefill function to return private information about the individuals and members of that individual's household. This also generated an Application for Insurance PDF that disclosed the personal information of these individuals, including DLNs. If the individual purchased a policy, their DLN and other personal information also appeared in their newly created user account.

12. On January 19, 2021 – almost two months later – a Metromile employee noticed a surge in abandoned quote applications. After determining that this surge of quotes were all being abandoned at the same point in the flow, Metromile investigated and determined that prefilled DLNs and other information could be viewed in plaintext on the face of the website. Over the next few days, Metromile made code changes that obfuscated the DLNs on the face of the Auto Quote Tool and in the website source code.

13. On January 24, 2021, an employee noticed a different attack involving exposed DLNs in the draft policy application PDF. Metromile staff blocked this attack and an additional attack on new customer account information.

14. After these attacks were terminated, Metromile staff set up various attack prevention and detection mechanisms, including geo-fencing, reCAPTCHA, and log monitoring. Metromile also hired a Chief Security Officer, added new security processes, and implemented frequent security training.

15. From the time that attackers began to exploit Metromile's systems until Metromile effectively foreclosed the ability to access additional DLNs, attackers were able to access and obtain the DLNs of approximately 90,000 New Yorkers.

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

16. Metromile failed to adopt reasonable safeguards to protect the private information of New Yorkers that it licensed and transmitted through its computer systems via the quoting

tool. This enabled threat actors to harvest tens of thousands of DLNs from Metromile's systems.

17. Metromile's did not perform risk assessments to assess the potential risks of handling private information within its public-facing web applications. As a result, Metromile did not identify these design failures and take steps to protect consumer's private information. Metromile also did not have reasonable penetration testing of public facing applications in place before these attacks. .

18. Metromile also did not use basic web application firewall tools and security information and event management tools to prevent and detect attacks, such as rate limiting, rate monitoring, IP logging, and log analysis. Without these common protections, the attack could have continued indefinitely without raising any alarm to Metromile information security.

19. Metromile also did not employ any mechanisms to deter automated traffic from its instant quote application, such as reCAPTCHA.

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

Respondent's Conduct Violated New York Law

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

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

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

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

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

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

RELIEF

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

a. "API" means application programming interface.

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

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

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

combination with a password or security question and answer that would permit access to an online account.

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

GENERAL COMPLIANCE

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

INFORMATION SECURITY PROGRAM

28. Respondent shall maintain a comprehensive information security program (“Information Security Program”) that is reasonably designed to protect the security, integrity, and confidentiality of Private Information that Respondent collects, uses, stores, retrieves, transmits, displays, maintains and/or otherwise processes. Respondent shall document in writing the content, implementation, and maintenance of the Information Security Program. The Information Security Program shall, at a minimum, include all the requirements detailed in paragraphs 31- 38 and the following processes:

- a. Assess, update, and document, not less than annually, internal and external risks to the security, integrity and confidentiality of Private Information, including but not limited to all entries in the most recent Data Inventory (as defined in paragraph 31, *infra*);
- b. Design, implement, and maintain reasonable administrative, technical, and physical safeguards to control the internal and external risks Respondent identified that are appropriate to: (i) the size and complexity of Respondent’s operations; (ii) the nature

and scope of Respondent's activities; and (iii) the volume and sensitivity of the Private Information that Respondent collects, uses, stores, retrieves, transmits, displays, maintains and/or otherwise processes;

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

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

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

29. Respondent shall designate a qualified employee responsible for implementing, maintaining, assessing, updating, and monitoring the Information Security Program (the "Chief Information Security Officer"). The Chief Information Security Officer shall have the credentials, background, and expertise in information security appropriate to the level, size, and complexity of their role in implementing, maintaining, assessing, updating, and monitoring the Information Security Program. The Chief Information Security Officer shall report at least quarterly to Respondent's Chief Executive Officer (or the equivalent thereof) and at least semi-annually to the Board of Directors (or an appropriately designated Board Committee) concerning Respondent's Information Security Program. Such reports shall be in writing and include but not

be limited to the following: the staffing and budgetary sufficiency of the Information Security Program, the degree to which the Information Security Program has been implemented, challenges to the success of the Information Security Program, the existing and emerging security risks faced by Respondent, and any barriers to the success of the Information Security Program.

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

SPECIFIC INFORMATION SECURITY REQUIREMENTS

31. Data Inventory: Within ninety (90) days of the Effective Date of this Assurance, to the extent it has not already done so, Respondent shall develop and maintain a data inventory of all instances in which it collects, uses, stores, retrieves, transmits, displays, maintains and/or otherwise processes Private Information. Respondent shall update and document its data inventory not less than annually. The data inventory shall, at a minimum, include the processes listed below.

- a. Identify all points at which Private Information is collected, used, stored, retrieved, transmitted, displayed, maintained, or otherwise processed;
- b. Map and/or track the complete path of all data flows involving Private

Information, including API calls; and

c. Ensure that reasonable safeguards are used to protect Private Information at all times, including but not limited to appropriate encryption, masking, obfuscation, and other methods of rendering Private Information incomprehensible and/or inaccessible.

32. Governance: Respondent shall maintain reasonable written policies and procedures designed to ensure the security, integrity, and confidentiality of Private Information obtained from a third party, including, but not limited to, prefill data providers.

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

a. Wherever Private Information is implicated by the regular and expected use of any such application, Respondent shall consider the privacy impact at each relevant stage of the software development lifecycle process;

b. Wherever Private Information is implicated by the regular and expected use of any such application, Respondent shall include reasonably designed privacy testing and documented approval each time the application is changed or updated;

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

d. For external software development vendors, evaluate, assess, and test adherence to Respondent's secure development procedures, guidelines, and standards or reasonably equivalent secure development standards.

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

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

36. Monitoring: Respondent 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.

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

- a. Promptly investigate and monitor for suspicious activity any platforms or applications operated by or on behalf of Respondent and any places on its Network that collect, use, store, retrieve, transmit, display, or maintain, or otherwise process Private Information; monitoring shall be at a level that is sufficiently granular to detect a potential Security Event;
- b. Promptly conduct a reasonable investigation to determine, at a minimum, whether Private Information is exposed or otherwise at risk; and
- c. Promptly implement changes necessary to protect Private Information at risk.

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

OAG ACCESS TO RECORDS

39. Respondent shall retain any documentation and reports required by paragraphs 27-37 for at least six years. Such documentation and reports shall be made available to the OAG within fourteen (14) days of a written request from the OAG. 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

40. Respondent shall pay to the State of New York two million dollars (\$2,000,000) 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. 25-042.

MISCELLANEOUS

41. Respondent expressly agrees and acknowledges that the OAG may initiate a subsequent investigation, civil action, or proceeding to enforce this Assurance, for violations of the Assurance, or if the Assurance is voided pursuant to paragraph 48, and agrees and acknowledges that in such event:

- a. any statute of limitations or other time-related defenses are tolled from and after the effective date of this Assurance;
- b. the OAG may use statements, documents or other materials produced or provided by the Respondent prior to or after the effective date of this Assurance;
- c. any civil action or proceeding must be adjudicated by the courts of the State of New York, and that Respondent irrevocably and unconditionally waives any objection to such action or proceeding based upon personal jurisdiction, inconvenient forum, or venue. Metromile does not concede that it is subject to New York jurisdiction other than with respect to the terms of this Assurance;
- d. evidence of a violation of this Assurance shall constitute prima facie proof of a violation of the applicable law pursuant to Executive Law § 63(15).

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

expenses, and court costs.

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

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

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

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

47. All notices, reports, requests, and other communications pursuant to this Assurance must reference Assurance No. 25-042, 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:

Scott Fischer, or in his absence, to the person holding the title of

General Counsel
Metromile LLC
5 Crosby Street, New York, New York 10013
legal@lemonade.com

If to the OAG, to:

The person holding the title of Bureau Chief, Bureau of Internet & Technology.

Office of the Attorney General
28 Liberty Street
New York, New York 10011

48. The OAG has agreed to the terms of this Assurance based on, among other things, the representations made to the OAG by the Respondent and their counsel and the OAG's own factual investigation as set forth in Findings, paragraphs 1-23 above. The Respondent represents and warrants that neither it nor its counsel has made any material representations to the OAG that are inaccurate or misleading. If any material representations by Respondent or its counsel are later found to be inaccurate or misleading, this Assurance is voidable by the OAG in its sole discretion.

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

50. The Respondent represents and warrants, through the signatures below, that the terms and conditions of this Assurance are duly approved. Respondent further represents and warrants that Metromile LLC, by Daniel Schreiber, the signatory to this AOD, is a duly authorized officer acting at the direction of the Board of Directors of Metromile LLC.

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

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

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

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

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

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

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

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

59. This Assurance may be executed in multiple counterparts by the parties hereto. All counterparts so executed shall constitute one agreement binding upon all parties,

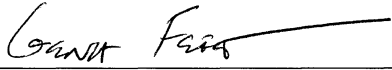
notwithstanding that all parties are not signatories to the original or the same counterpart. Each counterpart shall be deemed an original to this Assurance, all of which shall constitute one agreement to be valid as of the effective date of this Assurance. For purposes of this Assurance, copies of signatures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

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

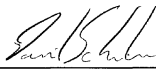
LETITIA JAMES
ATTORNEY GENERAL OF THE STATE OF
NEW YORK

Metromile LLC

By: _____


Gena Feist
Assistant Attorney General
Bureau of Internet & Technology
Office of the New York State
Attorney General
28 Liberty St.
New York, NY 10005

By: _____


Daniel Schreiber
Chief Executive Officer
Metromile LLC
5 Crosby Street
New York, New York 10013

Date: _____

10/8/25

Date: 2025-10-07