202-3196

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Lina M. Khan, Chair**
Rebecca Kelly Slaughter
Alvaro M. Bedoya
Melissa Holyoak
Andrew Ferguson

In the Matter of	**DECISION AND ORDER**
MOBILEWALLA, INC., a corporation,	**DOCKET NO. C-4811**

DECISION

The Federal Trade Commission ("Commission") initiated an investigation of certain acts and practices of the Respondent named in the caption. The Commission's Bureau of Consumer Protection ("BCP") prepared and furnished to Respondent a draft Complaint. BCP proposed to present the draft Complaint to the Commission for its consideration. If issued by the Commission, the draft Complaint would charge the Respondent with violations of the Federal Trade Commission Act.

Respondent and BCP thereafter executed an Agreement Containing Consent Order ("Consent Agreement"). The Consent Agreement includes: 1) statements by Respondent that it neither admits nor denies any of the allegations in the Complaint, except as specifically stated in this Decision and Order, and that only for purposes of this action, it admits the facts necessary to establish jurisdiction; and 2) waivers and other provisions as required by the Commission's Rules.

The Commission considered the matter and determined that it had reason to believe that Respondent has violated the Federal Trade Commission Act, and that a Complaint should issue stating its charges in that respect. The Commission accepted the executed Consent Agreement and placed it on the public record for a period of 30 days for the receipt and consideration of public comments. The Commission duly considered any comments received from interested persons pursuant to Section 2.34 of its Rules, 16 C.F.R. § 2.34. Now, in further conformity with the procedure prescribed in Rule 2.34, the Commission issues its Complaint, makes the following Findings, and issues the following Order:

Findings

1. The Respondent is Mobilewalla, Inc., a Delaware corporation with its principal office or place of business at 5170 Peachtree Road, Bldg 100, Suite 100, Chamblee, Georgia 30341.

2. The Commission has jurisdiction over the subject matter of this proceeding and over the Respondents, and the proceeding is in the public interest.

ORDER

Definitions

For purposes of this Order, the following definitions apply:

A. **"Affirmative Express Consent"** means any freely given, specific, informed, and unambiguous indication of an individual consumer's wishes demonstrating agreement by the individual, such as by an affirmative action, following a Clear and Conspicuous disclosure to the individual of: (1) the categories of information that will be collected; (2) the purpose(s) for which the information is being collected, used, or disclosed; (3) the hyperlink to a document that describes the types of entities to whom the information is disclosed; and (4) the hyperlink to a simple, easily-located means by which the consumer can withdraw consent and that Clearly and Conspicuously describes any limitations on the consumer's ability to withdraw consent. The Clear and Conspicuous disclosure must be separate from any "privacy policy," "terms of service," "terms of use," or other similar document.

The following do not constitute Affirmative Express Consent.

1. Inferring consent from the hovering over, muting, pausing, or closing of a given piece of content by the consumer; or

2. Obtaining consent through a user interface that has the substantial effect of subverting or impairing user autonomy, decision making, or choice.

B. **"Clear(ly) and conspicuous(ly)"** means that a required disclosure is difficult to miss (i.e., easily noticeable) and easily understandable by ordinary consumers, including in all of the following ways:

1. In any communication that is solely visual or solely audible, the disclosure must be made through the same means through which the communication is presented. In any communication made through both visual and audible means, such as a television advertisement, the disclosure must be presented simultaneously in both the visual and audible portions of the communication even if the representation requiring the disclosure ("triggering representation") is made through only one means.

2. A visual disclosure, by its size, contrast, location, the length of time it appears, and other characteristics, must stand out from any accompanying text or other visual elements so that it is easily noticed, read, and understood.

3. An audible disclosure, including by telephone or streaming video, must be delivered in a volume, speed, and cadence sufficient for ordinary consumers to easily hear and understand it.

4. In any communication using an interactive electronic medium, such as the Internet or software, the disclosure must be unavoidable.

5. The disclosure must use diction and syntax understandable to ordinary consumers and must appear in each language in which the triggering representation appears.

6. The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices and face-to-face communications.

7. The disclosure must not be contradicted or mitigated by, or inconsistent with, anything else in the communication.

8. When the representation or sales practice targets a specific audience, such as children, the elderly, or the terminally ill, "ordinary consumers" includes reasonable members of that group.

C. "**Convert**" means to use technical measures to Deidentify data and does not include associating other information to such data.

D. "**Covered Incident**" means any instance of a violation Provision I, II, III, IV or V of this Order.

E. **"Covered Information"** means information from or about an individual consumer including, but not limited to: (1) a first and last name; (2) Location Data; (3) an email address or other online contact information; (4) a telephone number; (5) a Social Security number; (6) a driver's license or other government-issued identification number; (7) a financial institution account number; (8) credit or debit card information; (9) a persistent identifier, such as a customer number held in a "cookie," a static Internet Protocol ("IP") address, a mobile device ID, or processor serial number; or (10) socio-economic or demographic data. Deidentified information is not Covered Information.

F. "**Data Product**" means any model, algorithm, derived data, or other tool in Respondent's custody or control developed using Historic Location Data. Data Product includes but is not limited to any derived data produced via inference (manual or automated) or predictions, such as audience segments.

G. **"Deidentified" or "Deidentifiable"** means information that cannot reasonably identify, relate to, describe, be associated with, or be linked, directly or indirectly, to a particular person, in that Respondent must, at a minimum:

1. Have implemented technical safeguards that prohibit reidentification of the person to whom the information pertains;

2. Have implemented business processes that specifically prohibit reidentification of the information;

3. Have implemented business processes to prevent inadvertent release of Deidentified information; and

4. Make no attempt to reidentify the information.

Location Data that is linked to a mobile advertising identifier or an individual's home address is not Deidentified.

H. "**Historic Location Data**" means any Location Data for which Respondent or its Supplier cannot demonstrate that consumers provided their consent in accordance with Provision VI.B (including Affirmative Express Consent) for Respondent's acquisition, transfer, and use of such Location Data.

I. "**Location Data**" means any data that may reveal a mobile device or consumer's precise location, including but not limited to Global Positioning System (GPS) coordinates, fine location data, cell tower information, or precise location information inferred from basic service set identifiers (BSSIDs), WiFi Service Set Identifiers (SSID) information, or Bluetooth receiver information, and any unique persistent identifier combined with any such data, such as a mobile advertising identifier (MAID) or identifier for advertisers (IDFA). Data that reveals only a mobile device or consumer's coarse location (e.g., zip code or census block location with a radius of at least 1,850 feet) or that is collected outside the United States and used for National Security purposes conducted by federal agencies or other federal entities is not Location Data.

J. **"National Security"** means the national defense, foreign intelligence and counterintelligence, international and internal security, and foreign relations. This includes countering terrorism; combating espionage and economic espionage conducted for the benefit of any foreign government, foreign instrumentality, or foreign agent; enforcing export controls and sanctions; and disrupting cyber threats that are perpetrated by nation states, terrorists, or their agents or proxies.

K. "**Respondent**" means Mobilewalla, Inc., a corporation, and its successors and assigns.

L. "**Sensitive Location**" means locations within the United States associated with: (1) medical facilities (e.g., family planning centers, general medical and surgical hospitals, offices of physicians, offices of mental health physicians and practitioners, residential mental health and substance abuse facilities, outpatient mental health and substance abuse centers, outpatient care

centers, psychiatric and substance abuse hospitals, and specialty hospitals); (2) religious organizations; (3) correctional facilities; (4) labor union offices; (5) locations held out to the public as predominantly providing education or childcare services to minors; (6) locations held out to the public as predominantly providing services to LGBTQ+ individuals such as service organizations, bars and nightlife; (7) locations held out to the public as predominantly providing services based on racial or ethnic origin; or (8) locations held out to the public as predominantly providing temporary shelter or social services to homeless, survivors of domestic violence, refugees, or immigrants; (9) locations of public gatherings of individuals during political or social demonstrations, marches, and protests; or (10) military installations, offices, or buildings.

M. "**Sensitive Location Data**" means any consumer Location Data associated with a Sensitive Location.

N. **"Supplier"** means a third-party from whom Respondent acquires Location Data and does not include a third-party that provides solely Location Data collected outside the United States for Respondent's use solely outside the United States.

Provisions

I. Prohibition Against Misrepresentations

IT IS ORDERED that Respondent, and Respondent's officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with the advertising, promotion, offering for sale, sale, or distribution any product or service, must not misrepresent in any manner, expressly or by implication:

A. The extent to which Respondent collects, uses, maintains, discloses, or deletes any Covered Information; and

B. The extent to which Location Data that Respondent collects, uses, maintains, or discloses is Deidentified.

II. Prohibition on Collection and Retention of Covered Information from Advertising Auctions

IT IS FURTHER ORDERED that Respondent and Respondent's officers, agents, employees, and attorneys, whether acting directly or indirectly, must not collect, purchase, or otherwise acquire or retain Covered Information that Respondent accesses while participating in online advertising auctions for any other purpose than participating in such auctions.

III. Prohibition on the Use, Sale, or Disclosure of Sensitive Location Data

IT IS FURTHER ORDERED that Respondent and Respondent's officers, agents, employees, and attorneys, whether acting directly or indirectly, must not sell, license, share, disclose, transfer, or otherwise use in any products or services Sensitive Location Data

associated with the Sensitive Locations that Respondent has identified within 180 days of this Order as part of the Sensitive Location Data Program established and maintained pursuant to Provision IV below.

Provided, however, that the prohibitions in this Provision III do not apply if Respondent uses Sensitive Location Data to Convert such data into data that (a) is not Sensitive Location Data or (b) is not Location Data.

IV. Sensitive Location Data Program

IT IS FURTHER ORDERED that Respondent, within 180 days of the issuance of this Order, must establish and implement, and thereafter maintain, a Sensitive Location Data Program (a) that develops a comprehensive list of Sensitive Locations using methods, sources, products or services developed by Respondent or offered by third parties and (b) that is designed to prevent the use, sale, licensing, transfer, or disclosure of Sensitive Location Data as provided in Provision III above. To satisfy this requirement, Respondent must, at a minimum:

A. Document in writing the components of the Sensitive Location Data Program as well as the plan for implementing and maintaining the Sensitive Location Data Program;

B. Identify a senior officer, such as a Chief Privacy Officer or Chief Compliance Officer, to be responsible for the Sensitive Location Data Program. The senior officer will be approved by and report directly to the board of directors or a committee thereof or, if no such board or equivalent body exists, to the principal executive officer of Respondent;

C. Provide the written program and any evaluations thereof or updates thereto to Respondent's board of directors or governing body or, if no such board or equivalent body exists, to the principal executive officer of Respondent at least every twelve months;

D. Develop and implement procedures to identify Sensitive Locations using methods, sources, products or services developed by Respondent or offered by third parties designed to be used by Respondent in preventing the sale, license, transfer, use, or other sharing or disclosure of Sensitive Location Data as provided in Provision III above. If a building or place is identified as including both a Sensitive Location and a non-Sensitive Location, Respondent may associate Location Data with the non-Sensitive Location only;

E. Assess, update, and document, at least once every six months, the accuracy and completeness of Respondent's list of Sensitive Locations. Such assessments must include:

1. Verifying that Respondent's list includes Sensitive Locations known to Respondent;

2. Identifying and assessing methods, sources, products, and services developed by Respondent or offered by third parties that identify Sensitive Locations;

3. Updating its list of Sensitive Locations by selecting and using the methods, sources, products, or services developed by Respondent or offered by third parties that are accurate and comprehensive in identifying Sensitive Locations; and

4. Documenting each step of this assessment, including the reasons Respondent selected the methods, sources, products, or services used in updating Respondent's list of Sensitive Locations.

F. Implement policies, procedures, and technical measures designed to prevent Respondent from using, selling, licensing, transferring, or otherwise sharing or disclosing Sensitive Location Data as provided in Provision III and monitor and test the effectiveness of these policies, procedures, and technical measures at least once every six months. Such testing must be designed to verify that Respondent is not using, selling, licensing, transferring, or otherwise sharing or disclosing Sensitive Location Data except as provided in Provision III above.

G. Initiate the process of deleting or rendering non-sensitive Sensitive Location Data associated with locations included in the list developed pursuant to Provision IV.D within 7 days of adding the location to the list of Sensitive Locations, except where retention is needed to fulfill an allowed purpose as provided in Provision III above; and

H. Evaluate and adjust the Sensitive Location Data Program in light of any changes to Respondent's operations or business arrangements, or any other circumstance that Respondent knows or has reason to know may have an impact on the Sensitive Location Data Program's effectiveness. At a minimum, Respondent must evaluate the Sensitive Location Data Program every twelve months and implement modifications based on the results.

V. Prohibition on the Sale, Licensing, or Disclosure of Private Residence Data

IT IS FURTHER ORDERED that Respondent and Respondent's officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, must not sell, license, or disclose Location Data that may determine the identity or the location of an individual's private residence (e.g., single family homes, apartments, condominiums, townhomes).

VI. Supplier Assessment Program

IT IS FURTHER ORDERED that that Respondent, within 90 days of the effective date of this Order, must implement a program designed to ensure that consumers have provided consent for the collection and use of Location Data obtained by Respondent, including by implementing and maintaining a Supplier Assessment Program. In connection with the Supplier Assessment Program, Respondent must, at a minimum:

A. Document in writing the content, implementation, and maintenance of the Supplier Assessment Program;

B. Conduct an initial assessment within 30 days of a Supplier entering into data-sharing agreements with Respondent (or, for parties with existing data-sharing agreements, within 60 days of the effective date of this Order), and thereafter annually, designed to confirm that consumers provide Affirmative Express Consent if feasible, or to confirm that consumers specifically consent to the collection, use, and sharing of their Location Data;

C. Create and maintain records of the Supplier's responses obtained by Respondent as provided in Provision VI.B above; and

D. Cease using, selling, licensing, transferring, or otherwise sharing or disclosing Location Data for which consumers have not provided consent, as provided in Provision VI.B above.

VII. Disclosures to Consumers

IT IS FURTHER ORDERED that:

A. Respondent and Respondent's officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, must provide a Clear and Conspicuous means for consumers to request the identity of any entity, business, or individual to whom Respondent has sold, transferred, licensed, or otherwise disclosed their Location Data during the one year period preceding the request.

B. Respondent may require consumers to provide Respondent with information reasonably necessary to complete such requests and to verify their identity, but must not use, provide access to, or disclose any information collected for such a request for any other purpose.

VIII. Withholding and Withdrawing Consent

IT IS FURTHER ORDERED that Respondent and Respondent's officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, must:

A. Provide a simple, easily-located means for consumers to withdraw any consent provided in accordance with Provision VI.B (including Affirmative Express Consent) provided to Respondent in connection with Location Data that is no more burdensome than the means by which the consumer provided consent. Such means may include a Clear and Conspicuous notice or link to an applicable website, operating system, device, or app permission or setting; and

B. Not unreasonably limit a consumer's ability to withhold or withdraw any consent provided in accordance with Provision VI.B (including Affirmative Express Consent) in connection with Location Data, such as by degrading the quality or functionality of a product or service as a penalty for withholding or withdrawing such consent, unless the collection and use of Location Data is technically necessary to provide the quality or functionality of the product or service without such degradation.

IX. Obligations When Consent is Withdrawn

IT IS FURTHER ORDERED that Respondent and Respondent's officers, agents, employees, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, must delete all Location Data

associated with a consumer or device within 30 days after Respondent receives notice that the consumer withdraws their consent using the means that Respondent provided under Provision VIII.A and immediately cease further collection or use of Location Data associated with that consumer or device, unless the consumer subsequently provides consent in accordance with Provision VI.B (including Affirmative Express Consent).

Provided, however, that such Location Data may be retained

i. to prevent, detect, or investigate data security incidents, or to protect against malicious, deceptive, fraudulent, or illegal activity directed at Respondent, for the shortest time reasonably necessary to fulfill this purpose, but Respondent must not use, provide access to, or disclose such Location Data retained for security and anti-fraud purposes, for any other purpose;

ii. if it is stored in Respondent's backups or archives that are not readily accessible ("Archived Location Data"), provided that (a) Respondent does not use, provide access to, or disclose Archived Location Data, (b) Archived Location Data is deleted in accordance with the data retention limits in Provision XI, and (c) Respondent deletes Archived Location Data pursuant to Provision IX if Respondent uses or provides access to Archived Location Data; or

iii. if Respondent is required to retain such Location Data to the extent requested by a government agency in a formal preservation letter that identifies the data to be preserved, or required by compulsory process, or otherwise required by law, regulation, or court order, and Respondent does not use such retained Location Data for any other purpose.

X. Location Data Deletion Requests

IT IS FURTHER ORDERED that Respondent and Respondent's officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, must:

A. Provide a Clear and Conspicuous means for consumers to request deletion of their device's Location Data held, stored, or under the control of Respondent. Respondent may require consumers to provide Respondent with any information necessary to complete such requests, but must not use, provide access to, or disclose any information collected for a deletion request for any other purpose, *provided, however*, that such Location Data may be retained:

i. to prevent, detect, or investigate data security incidents, or to protect against malicious, deceptive, fraudulent, or illegal activity directed at the Respondent, for the shortest time reasonably necessary to fulfill this purpose, but Respondent must not use, provide access to, or disclose such Location Data retained for security and anti-fraud purposes, for any other purpose; or

ii. if it is stored in Respondent's backups or archives that are not readily accessible ("Archived Location Data"), provided that (a) Respondent does not use, provide access to, or disclose Archived Location Data, (b) Archived Location Data is deleted in accordance with the data retention limits in Provision XI, and (c) Respondent deletes Archived Location Data pursuant to Provision X if Respondent uses or provides access to Archived Location Data; or

iii. if Respondent is required to retain such Location Data to the extent requested by a government agency in a formal preservation letter that identifies the data to be preserved, or required by compulsory process, or otherwise required by law, regulation, or court order, and Respondent does not use such retained Location Data for any other purpose.

B. Create and maintain a process by which Respondent's Suppliers may provide Respondent with notice of consumers' deletion requests.

XI. Data Retention Limits

IT IS FURTHER ORDERED that Respondent, in connection with the collection, maintenance, use, or disclosure of, or provision of access to, Covered Information, must:

A. Within 60 days of effective date of this Order, document, adhere to, and make publicly available through a link on the home page of their website(s), in a manner that is Clear and Conspicuous, a retention schedule for Covered Information, setting forth: (1) the purpose or purposes for which each type of Covered Information is collected or used; (2) the specific business needs for retaining each type of Covered Information; and (3) an established timeframe for deletion of each type of Covered Information limited to the time reasonably necessary to fulfill the purpose for which the Covered Information was collected, and in no instance providing for the indefinite retention of any Covered Information;

B. Within 60 days of the effective date of this Order, Respondent shall provide a written statement to the Commission, pursuant to the Provision entitled Compliance Report and Notices, describing the retention schedule for Covered Information made publicly available on its website(s); and

C. Prior to collecting or using any new type of Covered Information related to consumers that was not being collected as of the issuance date of this Order, and is not described in retention schedules published in accordance with sub-Provision A of this Provision, Respondent must update its retention schedule setting forth: (1) the purpose or purposes for which the new information is collected; (2) the specific business needs for retaining the new information; and (3) a set timeframe for deletion of the new information that precludes indefinite retention.

XII. Deletion

IT IS FURTHER ORDERED that Respondent and Respondent's officers, agents, employees, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, must, unless prohibited by law:

A. Within 90 days after the effective date of this Order, delete or destroy all Historic Location Data and consumers' unhashed and hashed phone numbers, and provide a written statement to the Commission, pursuant to Provision XV, confirming that all such information has been deleted or destroyed;

B. Within 120 days after the effective date of this Order, delete or destroy all Data Products, and provide a written statement to the Commission, pursuant to Provision XV, confirming such deletion or destruction; and

C. Within 90 days after the effective date of this Order, (i) inform Respondent's customers that received Historic Location Data within 3 years prior to the issuance date of this Order, of the FTC's requirement in Provisions XII.A and XII.B that the FTC requires such data to be deleted, Deidentified, or rendered non-sensitive, unless such customer has obtained records in accordance with Provision VI.B showing that the relevant consumer consented to the collection, use, and sharing of their Historic Location Data, and (ii) Respondent shall promptly submit, within 10 days of sending to its customers, all such notices to the Commission under penalty of perjury as specified in the Provision of this Order titled "Compliance Report and Notices."

Provided however, Respondent shall not be required to comply with Provisions XII.A. and XII.B., if:

1. within 90 days of the effective date of this Order,

    a. Respondent has obtained records in accordance with Provision VI.B showing that consumers consented to the collection, use, and sharing of their Historic Location Data; or

    b. the Historic Location Data is Deidentified or rendered non-sensitive in accordance with Provision III above, and provided that Historic Location Data is subject to the obligations in Provision IV above; or

2. the Historic Location Data is retained to prevent, detect, or investigate data security incidents, or to protect against malicious, deceptive, fraudulent, or illegal activity directed at the Respondent, for the shortest time reasonably necessary to fulfill this purpose, but Respondent must not use, provide access to, or disclose such Historic Location Data retained for security and anti-fraud purposes, for any other purpose; or

3. if Respondent is required to retain such Historic Location Data to the extent requested by a government agency in a formal preservation letter that identifies the data to be preserved, or required by compulsory process, or otherwise required by law, regulation, or court order and Respondent does not use such retained Historic Location Data for any other purpose.

XIII. Mandated Privacy Program

IT IS FURTHER ORDERED that Respondent, for any business that Respondent controls directly or indirectly, in connection with the collection, maintenance, use, or disclosure of, or provision of access to, Covered Information, must establish and implement, and thereafter maintain, a comprehensive privacy program (the "Program") that protects the privacy of such Covered Information. Respondent must comply with this provision within 60 days of effective date of this Order. To satisfy this requirement, Respondent must at a minimum:

A. Document in writing the content, implementation, and maintenance of the Program;

B. Provide the written Program and any evaluations thereof or updates thereto to Respondent's board of directors or, if no such board or equivalent governing body exists, to a senior officer of the Respondent responsible for the Program at least once every twelve months;

C. Designate a qualified employee or employees to coordinate and be responsible for the Program;

D. Assess and document, at least every 12 months, internal and external risks to the privacy of Covered Information that could result in the unauthorized collection, maintenance, use, disclosure, alteration, destruction of, or provision of access to Covered Information;

E. Design, implement, maintain, and document safeguards that control for the material internal and external risks Respondent identifies to the privacy of Covered Information identified in response to Provision XIII.D. Each safeguard must be based on the volume and sensitivity of Covered Information that is at risk, and the likelihood that the risk could be realized and result in the unauthorized collection, maintenance, use, disclosure, alteration, or destruction of, or provision of access to Covered Information.

F. On at least an annual basis, provide privacy training programs for all employees and independent contractors responsible for handling or who have access to Covered Information, updated to address any identified material internal or external risks and safeguards implemented pursuant to this Order;

G. Test and monitor the effectiveness of the safeguards at least once every twelve (12) months, and modify the Program based on the results; and

H. Evaluate and adjust the Program in light of any changes to Respondent's operations or business arrangements, new or more efficient technological or operational methods to control for the risks identified in Provision XIII.D of this Order, or any other circumstances that Respondent knows or has reason to believe may have an impact on the effectiveness of the Program or any of its individual safeguards. At a minimum, Respondent must evaluate the Program at least once every 12 months and modify the Program based on the results.

XIV. Acknowledgments of the Order

IT IS FURTHER ORDERED that Respondent obtains acknowledgments of receipt of this Order:

A. Respondent, within 10 days after the effective date of this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.

B. For 10 years after the issuance date of this Order, Respondent must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees having managerial responsibilities for conduct related to the subject matter of the Order and all agents and representatives who participate in conduct related to the subject matter of the Order; and (3) any business entity resulting from any change in structure as set forth in the Provision titled Compliance Report and Notices. Delivery must occur within 10 days after the effective date of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.

C. From each individual or entity to which Respondent delivered a copy of this Order, Respondent must obtain, within thirty (30) days, a signed and dated acknowledgment of receipt of this Order.

XV. Compliance Report and Notices

IT IS FURTHER ORDERED that Respondent makes timely submissions to the Commission:

A. One year after the issuance date of this Order, Respondent must submit a compliance report, sworn under penalty of perjury, in which Respondent must: (a) identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission, may use to communicate with Respondent; (b) identify all of Respondent's businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (c) describe the activities of each business, including the goods and services offered, the means of advertising, marketing, and sales; (d) describe in detail whether and how Respondent is in compliance with each Provision of this Order, including a discussion of all of the changes the Respondent made to comply with the Order; and (e) provide a copy of each Acknowledgment of the Order obtained pursuant to this Order, unless previously submitted to the Commission.

B. For 10 years after the date of this Order, Respondent must submit a compliance notice, sworn under penalty of perjury, within 14 days of any change in the following: (a) any designated point of contact; or (b) the structure of Respondent, or any entity that Respondent has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order.

C. Respondent must submit notice of the filing of any bankruptcy petition, insolvency

proceeding, or similar proceeding by or against such Respondent within 14 days of its filing.

D. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: "I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____" and supplying the date, signatory's full name, title (if applicable), and signature.

E. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: In re Mobilewalla, Inc. [*the C or D docket number*].

XVI. Recordkeeping

IT IS FURTHER ORDERED that Respondent must create certain records for 10 years after the issuance date of the Order, and retain each such record for 5 years, unless otherwise specified below. Specifically, Respondent must create and retain the following records:

A. Accounting records showing the revenues from all goods or services sold, the costs incurred in generating those revenues, and resulting net profit or loss;

B. Personnel records showing, for each person providing services in relation to any aspect of the Order, whether as an employee or otherwise, that person's: name; addresses; telephone numbers; job title or position; dates of service; and (if applicable) the reason for termination;

C. Copies or records of all consumer complaints that relate to the collection, use, maintenance, or disclosure of Covered Information, whether received directly or indirectly by Respondent, such as through a third party, and any response;

D. For 5 years from the date received, copies of all subpoenas and other communications with law enforcement or other government agencies, or entities Respondent knows or should know is contracted by or otherwise working with a law enforcement or other government agency with respect to that subpoena or communication, if such communication relates to Respondent's compliance with this Order, including Respondent's collection, use, or transfer of Covered Information;

E. A copy of each widely disseminated representation by Respondent that describes the extent to which Respondent maintains or protects the privacy, security and confidentiality of any Covered Information, including any representation concerning a change in any website or other service controlled by Respondent that relates to the privacy, security, and confidentiality of Covered information;

F. Records showing Respondent's implementation of the Supplier Assessment Program required by Provision VI;

G. Records showing Respondent's implementation of policies, controls, and technical measures to prevent the collection, or use of Sensitive Location Data prohibited by Provision III; and

H. All records necessary to demonstrate full compliance with each Provision of this Order, including all submissions to the Commission.

XVII. Compliance Monitoring

IT IS FURTHER ORDERED that, for the purpose of monitoring Respondent's compliance with this Order:

A. Within 14 days of receipt of a written request from a representative of the Commission, Respondent must: submit additional compliance reports or other requested information, which must be sworn under penalty of perjury, and produce records for inspection and copying.

B. For matters concerning this Order, representatives of the Commission are authorized to communicate directly with Respondent. Respondent must permit representatives of the Commission to interview anyone affiliated with Respondent who has agreed to such an interview. The interviewee may have counsel present.

C. The Commission may use all other lawful means, including posing through its representatives as consumers, suppliers, or other individuals or entities, to Respondent or any individual or entity affiliated with Respondent, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

XVIII. Order Effective Dates

IT IS FURTHER ORDERED that this Order is final and effective upon the date of its publication on the Commission's website (ftc.gov) as a final order. This Order will terminate 20 years from the date of its issuance (which date may be stated at the end of this Order, near the Commission's seal), or 20 years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of this Order, whichever comes later; *provided, however,* that the filing of such a complaint will not affect the duration of:

A. Any Provision in this Order that terminates in less than 20 years;

B. This Order's application to any Respondent that is not named as a defendant in such complaint; and

C. This Order if such complaint is filed after the Order has terminated pursuant to this Provision.

Provided, further, that if such complaint is dismissed or a federal court rules that the Respondent did not violate any Provision of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order will terminate according to this Provision as though the complaint had never been filed, except that the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission, Commissioner Holyoak dissenting.

April J. Tabor
Secretary

SEAL:
ISSUED: January 13, 2025