UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF IDAHO

FEDERAL TRADE COMMISSION, Plaintiff, v. KOCHAVA, INC., Defendant.	Case No. 2:22-cv-00377-BLW **STIPULATED ORDER FOR INJUNCTION AND OTHER RELIEF**

Plaintiff, the Federal Trade Commission ("Commission"), filed its Complaint, subsequently amended on June 5, 2023 and amended again as Second Amended Complaint For Permanent Injunction and Other Relief on July 15, 2024 (as amended, "Complaint"), for a permanent injunction, and other relief in this matter, pursuant to Section 13(b) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 53(b). The Commission and Defendants stipulate to the entry of this Stipulated Order for Injunction and Other Relief ("Order") to resolve all matters in dispute in this action between them.

THEREFORE, IT IS ORDERED as follows:

FINDINGS

1. This Court has jurisdiction over this matter.

2. The Complaint charges that Defendants participated in unfair acts or

practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45, in the use and disclosure of data gathered from consumers' mobile devices and other sources without consumers' knowledge or consent.

3. Defendants neither admit nor deny any of the allegations in the Complaint, except as specifically stated in this Order. Only for purposes of this action, Defendants admit the facts necessary to establish jurisdiction.

4. Defendants waive any claim that they may have under the Equal Access to Justice Act, 28 U.S.C. § 2412, concerning the prosecution of this action through the date of this Order, and agree to bear their own costs and attorney fees.

5. Defendants and the Commission waive all rights to appeal or otherwise challenge or contest the validity of this Order.

DEFINITIONS

For the purpose 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) a hyperlink to a document that describes the types of entities to whom the Covered Information is disclosed;

and (4) a 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 does 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 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. **"Covered Information"** means information from or about an individual consumer including, but not limited to: (1) a first and last name; (2) Precise 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. Deidentified information is not Covered Information.

D. "**Deidentified**," "**Deidentifiable**," or "**Deidentify**" means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular person, in that Defendants must, at a minimum:

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

2. Have implemented business processes that specifically prohibit reidentification of the information, including by buyers, customers, or other entities to whom Defendants provide the information;

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

4. Make no attempt to reidentify the information.

E. "**Historical Location Data**" means any Precise Location Data that Defendants collected from consumers without consumers' Affirmative Express Consent prior to the entry of this Order.

F. "**National Security**" means 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.

G. "**Precise Location Data**" means any data that may reveal a mobile device's or consumer's precise location, including but not limited to Global Positioning System (GPS) coordinates, 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: (1) reveals only a mobile device's or consumer's coarse location data (e.g., zip code or census block location with a radius of at least 1,850 feet), or (2) is used for (a) Security Purposes, (b) National Security purposes conducted by federal agencies or other federal entities, or (c) response by a law enforcement agency to an imminent risk

of death or serious bodily harm to a person, is not Precise Location Data.

H. "**Recipient**" means an entity, business, or individual as to which a Defendant has knowledge that consumers' Precise Location Data was sold, transferred, licensed, or otherwise disclosed by a Defendant.

I. "**Defendant CDS**" means Collective Data Solutions, LLC, and its successors and assigns.

J. "**Defendant Kochava**" means Kochava Inc., and its successors and assigns.

K. "**Defendants**" means both Defendant Kochava and Defendant CDS.

L. "**Security Purposes**" means preventing, detecting, protecting against, or responding to data security incidents, including cybersecurity incidents, identity theft, fraud, phishing, harassment, malicious or deceptive activities, or preserving the integrity or security of systems.

M. "**Sensitive Locations**" means locations within the United States associated with:

(1) medical facilities; (2) religious organizations; (3) locations of entities held out to the public as predominantly providing education or childcare services to minors; (4) locations held out to the public as providing temporary shelter or social services to homeless, or survivors of domestic violence; or (5) military or federal law enforcement installations, offices, or buildings.

N. "**Sensitive Location Data**" means any consumer's Precise

Location Data associated with a Sensitive Location.

O. "**Supplier-Provided Location Data**" means any data that may reveal a mobile device's or consumer's precise location, including but not limited to Global Positioning System (GPS) coordinates, 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's or consumer's coarse location data (e.g., zip code or census block location with a radius of at least 1,850 feet) is not Supplier-Provided Location Data.

P. "**Third-Party Incident**" means the sharing by a third party of Defendants' Precise Location Data, in violation of a contractual requirement between Defendants and the third party.

ORDER

I. PROHIBITION AGAINST MISREPRESENTATIONS

IT IS ORDERED that Defendants and Defendants' officers, agents, employees, and allother 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

of any product or service, must not misrepresent, in any manner, expressly or by implication:

A. The extent to which Defendants review data suppliers' compliance and consent frameworks, consumer disclosures, sample notices, and opt-in controls;

B. The extent to which Defendants collect, use, maintain, disclose, or delete any Covered Information; and

C. The extent to which the Precise Location Data that Defendants collect, use, maintain, or disclose is Deidentified.

II. PROHIBITIONS ON THE SALE OR DISCLOSURE OF SENSITIVE LOCATION DATA

IT IS FURTHER ORDERED that Defendants and Defendants' officers, agents, and employees, whether acting directly or indirectly, must not sell, license, transfer, share, or disclose in any products or services Sensitive Location Data associated with the Sensitive Locations that Defendant CDS has identified within 90 days of the entry of this Order as part of the Sensitive Locations Data Program established and maintained pursuant to Provision III below.

Provided, however, that the prohibitions in this Provision II do not apply if Defendants have a direct relationship with the consumer related to the Sensitive Location Data, the consumer has provided Affirmative Express Consent, and the Sensitive Location Data is used to provide a service directly requested by the

consumer.

III. SENSITIVE LOCATION DATA PROGRAM

IT IS FURTHER ORDERED that Defendant CDS, within 90 days of the entry of this Order, must establish and implement, and thereafter maintain, a Sensitive Location Data Program to develop a comprehensive list of Sensitive Locations and to prevent the sale, licensing, transfer, sharing, or disclosure of Sensitive Location Data as provided in Provision II above. Defendant Kochava, before selling, licensing, transferring, sharing, or disclosing Precise Location Data, must comply with, and thereafter maintain, the requirements of this Provision, including all subparts.

To satisfy this requirement, Defendant CDS and, if applicable, Defendant Kochava 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 Defendant CDS and, if applicable,

Defendant Kochava;

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

D. Develop and implement procedures to identify Sensitive Locations to be used by Defendant CDS and, if applicable, Defendant Kochava in preventing the sale, license, transfer, or other sharing or disclosure of Sensitive Location Data as provided in Provision II above. If a building or place is identified as including both a Sensitive Location and a non-Sensitive Location, Defendants may associate Precise Location Data with the non-Sensitive Location only;

E. Assess, update, and document, at least once every three months, the accuracy and completeness of the list of Sensitive Locations. The assessments must include:

1. Verifying that the list includes Sensitive Locations known to Defendant CDS and, if applicable, Defendant Kochava;

2. Identifying and assessing methods, sources, products, and services developed by Defendant CDS and, if applicable, Defendant Kochava 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 Defendant CDS and, if applicable, Defendant Kochava or offered by third parties that are accurate and comprehensive in identifying Sensitive Locations;

4. Considering new categories of Sensitive Locations, not enumerated in the definition of Sensitive Locations. Defendant CDS and, if applicable, Defendant Kochava must determine whether to add the newly identified categories to the list of Sensitive Locations and, as applicable, complete these additions within the time frames specified in Section III.G; and

5. Documenting each step of this assessment, including the reasons Defendant CDS and, if applicable, Defendant Kochava, selected the methods, sources, products, or services used in updating the list of Sensitive Locations.

F. Implement policies, procedures, and technical measures designed to prevent Defendant CDS and, if applicable, Defendant Kochava from selling, licensing, transferring, or otherwise sharing or disclosing Sensitive Location Data as provided in Provision II above, and

monitor and test the effectiveness of these policies, procedures, and technical measures at least once every three months. Such testing must be designed to verify that Defendant CDS and, if applicable, Defendant Kochava are not selling, licensing, transferring, or otherwise sharing or disclosing Sensitive Location Data;

G. For any Sensitive Location Data for which consent has not been confirmed, as provided for in Provision VI.B below, initiate the process of deleting or rendering non-sensitive Sensitive Location Data associated with locations included in the list developed pursuant to Subparts D and E, within 2 days of determining that consumers have not provided consent, and complete the process within 30 days of initiation. The time period to complete this process may be extended by additional 30 day periods (not to exceed 90 total days) when reasonably necessary, provided Defendant CDS and, if applicable, Defendant Kochava document at each interval, the reasons for the extension and the progress made, and Defendant CDS and, if applicable, Defendant Kochava must not use, provide access to, or disclose Sensitive Location Data during the process of deleting or rendering non-sensitive, for any other purpose; and

H. Evaluate and adjust the Sensitive Location Data Program in light of any changes to operations or business arrangements, or any other circumstance that Defendant CDS and, if applicable, Defendant Kochava know or have reason to know may have an impact on the Sensitive Location Data Program's

effectiveness. At a minimum, Defendant CDS and, if applicable, Defendant Kochava must evaluate the Sensitive Location Data Program every twelve months and implement modifications based on the results.

IV. CUSTOMER NOTICE OBLIGATIONS

IT IS FURTHER ORDERED that Defendants, within 90 days of the entry of this Order, must provide their customers who received Precise Location Data within the past two years with a copy of this Order.

V. THIRD-PARTY INCIDENT REPORTS

IT IS FURTHER ORDERED that within 30 days of any Defendant's determination that a Third-Party Incident has occurred, Defendant must submit a report to the Commission. The report must include, to the extent possible:

A. The estimated date range when the Third-Party Incident occurred;

B. A description of the facts relating to the Third-Party Incident, including the causes of the Third-Party Incident, if known, and participants;

C. A description of each type of information that was affected by the Third-Party Incident;

D. The numbers of consumers whose information was affected by the Third-Party Incident;

E. The acts Defendant has taken to date to remediate the Third-Party Incident and protect Precise Location Data from further exposure or access; and

F. Unless otherwise directed by a Commission representative in writing, Defendant must submit all Third-Party Incident reports to the Commission under penalty of perjury as specified in the Section of this Order titled "Compliance Report and Notices."

VI. SUPPLIER ASSESSMENT PROGRAM

IT IS FURTHER ORDERED that Defendant CDS, within 90 days of the entry of this Order, must implement a program designed to confirm that consumers have provided consent for the collection and use of all Supplier-Provided Location Data obtained by Defendant CDS by implementing and maintaining a "Supplier Assessment Program." Defendant Kochava, before selling, using, licensing, transferring, sharing, or disclosing Supplier-Provided Location Data, must comply with, and thereafter maintain, the requirements of this Provision, including all subparts.

In implementing the Supplier Assessment Program, Defendant CDS and, if applicable, Defendant Kochava must, at a minimum:

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

B. Conduct an initial assessment either within 30 days of a third party entering into data sharing agreements with Defendant CDS and, if applicable, Defendant Kochava (or, for parties with existing data-sharing agreements, within

30 days of the entry of this Order) or within 30 days of the initial date of data collection from such a third party, and thereafter annually, designed: (i) to confirm, if available, that consumers provide Affirmative Express Consent, or (ii) to confirm that consumers specifically consent to the collection, use, and disclosure of all Supplier-Provided Location Data;

C. Create and maintain records of the suppliers' responses obtained by Defendant CDS and, if applicable, Defendant Kochava under the Supplier Assessment Program; and

D. Cease from using, selling, licensing, transferring, or otherwise sharing or disclosing all Supplier-Provided Location Data for which consumers' consent has not been confirmed by the Supplier Assessment Program, as provided in Provision VI.B above.

VII. DISCLOSURES TO CONSUMERS

IT IS FURTHER ORDERED that Defendant CDS and Defendant CDS'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 provide a Clear and Conspicuous means for consumers to request the identity of any Recipient. Defendant may require consumers to provide Defendant 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. Defendant Kochava and Defendant Kochava'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 comply with the requirements of this Provision if Defendant Kochava sells, licenses, transfers, shares, or discloses Precise Location Data.

Provided however, that the Disclosure requirements in this Provision VII do not apply if Defendant CDS and, if applicable, Defendant Kochava: (i) provides consumers with a Clear and Conspicuous method to submit a request to delete their Precise Location Data from the commercial databases of all Recipients of such Precise Location Data; (ii) expressly instructs (or contractually requires) such Recipients to honor such requests sent or made available to them by Defendant CDS and, if applicable, Defendant Kochava; (iii) expressly requests (or contractually demands) written confirmation of deletion of the identified Precise Location Data; and (iv) provides consumers with written confirmation of such deletion requests or instructions sent to such Recipients and written confirmation of deletion from such Recipients (where confirmed), no later than 90 days after the receipt of consumers' requests. Defendant CDS and, if applicable, Defendant Kochava may require consumers to provide Defendant 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. WITHDRAWING CONSENT

IT IS FURTHER ORDERED that Defendant CDS and Defendant CDS'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 provide a simple, easily located means for consumers to withdraw consent to Defendant CDS's use or disclosure of their device's Precise Location Data. Such means may include a Clear and Conspicuous notice or link to an applicable operating system or device setting. Defendant CDS may require consumers to provide Defendant CDS with information necessary to complete such requests, but Defendant CDS must not use, provide access to, or disclose any information collected for such a request for any other purpose. Defendant Kochava and Defendant Kochava'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 comply with the requirements of this Provision if Defendant Kochava sells, uses, licenses, transfers, shares, or discloses Precise Location Data.

IX. OBLIGATIONS WHEN CONSENT IS WITHDRAWN

IT IS FURTHER ORDERED that Defendants, and Defendants' 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 cease using and disclosing all Precise Location Data associated with a specific device within 30 days after Defendant CDS receives notice that the consumer has withdrawn their consent through the means required by Provision VIII above. Defendant Kochava and Defendant Kochava'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 comply with the requirements of this Provision if Defendant Kochava sells, uses, licenses, transfers, shares, or discloses Precise Location Data.

X. PRECISE LOCATION DATA DELETION REQUESTS

IT IS FURTHER ORDERED that Defendant CDS and Defendant CDS'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 implement and maintain a simple and Clear and Conspicuous means for consumers to request that Defendant CDS delete Precise Location Data that Defendant CDS previously collected about their mobile device, and delete such Precise Location Data within 30 days of receipt of such request unless a shorter period for deletion is required by law. Defendant CDS shall create and maintain a process by which a deletion request provided to Defendant CDS is treated as notice to its parent company.

Defendant CDS may require consumers to provide Defendant CDS with 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. Defendant Kochava and Defendant Kochava'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 comply with the requirements of this Provision if Defendant Kochava sells, uses, licenses, transfers, shares, or discloses Precise Location Data.

XI. DATA RETENTION LIMITS

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

A. Within 60 days of the entry 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. Defendant Kochava must comply with, and thereafter adhere to, the requirements of this Provision before selling,

using, licensing, transferring, sharing, or disclosing Covered Information.

B. Within 60 days of the entry of this Order, Defendants 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). Defendant Kochava must comply with, and thereafter adhere to, the requirements of this Provision before selling, using, licensing, transferring, sharing, or disclosing Covered Information.

C. Prior to collecting or using any new type of information related to consumers that was not being collected as of the entry of this Order, and is not described in retention schedules published in accordance with sub-Provision A of this Provision entitled Data Retention Limits, Defendant CDS and, if applicable, Defendant Kochava 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. Defendant Kochava must comply with, and thereafter adhere to, the requirements of this Provision if Defendant Kochava sells, uses, licenses, transfers, shares, or discloses Covered Information.

XII. DEIDENTIFICATION

IT IS FURTHER ORDERED that Defendants and Defendants' 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 entry of this Order, Deidentify or render non-sensitive,all Historical Location Data, and provide a written statement to the Commission, pursuant to Provision XV.D, confirming that all such information has been so Deidentified or rendered non-sensitive; and

B. Within 90 days after the entry of this Order, (i) inform Defendants' customers that received Historical Location Data within 2 years prior to the entry of this Order, of the FTC's requirement in Provision XII.A that the FTC requires such data to be Deidentified or rendered non-sensitive, and (ii) Defendants 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, Defendants shall have the option to retain Historical Location Data if Defendants have obtained records in accordance with Provision VI showing that consumers consented to the collection, use, and disclosure of their Historical Location Data, within 90 days after the entry of this Order.

XIII. MANDATED PRIVACY PROGRAM

IT IS FURTHER ORDERED that Defendants, and any business that Defendants controls directly or indirectly, in connection with the collection, maintenance, use, disclosure of, or provision of access to Covered Information, must, within 90 days of the entry of this Order, establish and implement, and thereafter maintain, a comprehensive privacy program (the "Program") that protects the privacy of such Covered Information. To satisfy this requirement, Defendants must at a minimum do the following:

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 Defendants' boards of directors or governing body or, if no such board or equivalent governing body exists, to a senior officer of each Defendant responsible for the Program at least once every 12 months;

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

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

E. Design, implement, maintain, and document safeguards that control

for the material internal and external risks Defendants identify 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 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 12 months, and modify the Program based on the results; and

H. Evaluate and adjust the Program in light of any changes to Defendants' 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 Defendants know or have reason to believe may have an impact on the effectiveness of the Program or any of their individual safeguards. At a minimum, Defendants 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 Defendants obtain acknowledgments of receipt of this Order:

A. Defendants, within 10 days after the entry of this Order, must submit to the Commission acknowledgments of receipt of this Order sworn under penalty of perjury.

B. For 5 years after the entry of this Order, Defendants 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 this Order, and all agents and representatives having managerial responsibilities for the conduct related to the subject matter of this Order; and (3) any business entity resulting from any change in structure as set forth in Provision XV titled Compliance Report and Notices. Delivery must occur within 10 days after the entry 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 Defendants delivered a copy of this Order, Defendants must obtain, within 30 days, a signed and dated acknowledgment of receipt of this Order.

XV. COMPLIANCE REPORT AND NOTICES

IT IS FURTHER ORDERED that Defendants make timely submissions to the Commission:

A. One year after the entry of this Order, Defendants must submit a

compliance report, sworn under penalty of perjury, in which Defendants must: (1) 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 Defendants; (2) identify all of Defendants' businesses (including without limitation any parent company, successor in interest, subsidiary, or spin-off) by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (3) describe the activities of each business, including the goods and services offered, the means of advertising, marketing, and sales; (4) describe in detail whether and how Defendants are in compliance with each Provision of this Order relevant to them, including a discussion of all of the changes Defendants made to comply with the Order; and (5) provide a copy of each Acknowledgment of the Order obtained pursuant to this Order, unless previously submitted to the Commission.

B. Defendants must submit a compliance notice, sworn under penalty of perjury, within 14 days of any change in the following: (1) any designated point of contact; or (2) the structure of Defendants or any entity that Defendants have 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. Defendants must submit notice of the filing of any bankruptcy

petition, insolvency proceeding, or similar proceeding by or against either Defendant 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 Collective Data Solutions, LLC.

XVI. RECORDKEEPING

IT IS FURTHER ORDERED that Defendants must create certain records for 5 years after the entry of the Order, and retain each such record for 5 years. Specifically, Defendants 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, 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 of all consumer complaints that relate to the collection, use, maintenance, or disclosure of Covered Information, whether received directly or indirectly, such as through a third party, and any response;

D. For 5 years from the date received, copies of communications from law enforcement, if such communications request information or documents relating to Defendants' compliance with this Order;

E. A copy of each widely disseminated representation by each of Defendants that describes the extent to which Defendants (i) review data suppliers' compliance and consent frameworks, consumer disclosures, sample notices, and opt-in controls; (ii) the extent to which Defendants collect, use, maintain, disclose, or delete any Covered Information; and (iii) the extent to which the Precise Location Data that Defendants collect, use, maintain, or disclose is Deidentified;

F. Records showing that Defendants have met the consent requirements set forth in Provision XII for retaining Historical Location Data;

G. Records showing Defendant CDS and, if applicable, Defendant

Kochava has met the applicable requirements of the Supplier Assessment Program required by Provision VI;

H. Records showing Defendant CDS and, if applicable, Defendant Kochava has met the applicable requirements of the Sensitive Location Data Program required by Provision III;

I. Records showing Defendant CDS and, if applicable, Defendant Kochava has met the applicable requirements related to the processing of consumer deletion requests as provided in Provision X; and

J. 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 Defendants' compliance with this Order:

A. Within 14 days of receipt of a written request from a representative of the Commission, Defendants 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 Defendants. Defendants must permit representatives of the Commission to interview anyone affiliated with Defendants 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 Defendants or any individual or entity affiliated with Defendants, 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 will terminate 10 years from the date it is entered by the Court.

XIX. RETENTION OF JURISDICTION

IT IS FURTHER ORDERED that this Court retains jurisdiction of this matter for purposes of construction, modification, and enforcement of this Order.

DATED: June 25, 2026

B. Lynn Winmill
U.S. District Court Judge