

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

FEDERAL TRADE COMMISSION,

Plaintiff,

v.

RING LLC,
A Delaware limited liability company,

Defendant.

CASE NO: 1:23-cv-1549

**[PROPOSED]
STIPULATED ORDER FOR
INJUNCTION AND MONETARY
JUDGMENT**

Plaintiff, the Federal Trade Commission (“Commission”), filed its Complaint for Injunction and Other Relief (“Complaint”) in this matter, pursuant to Section 13(b) of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. §§ 53(b). Defendant has waived service of the summons and the Complaint. Plaintiff and Defendant stipulate to the entry of this Stipulated Order for Injunction and Monetary Judgment (“Order”) to resolve all matters in dispute in this action between them without requiring the Commission to file an administrative complaint pursuant to 16 C.F.R. Part 3 and then seek monetary relief in federal court pursuant to Section 19(a)(2) of the FTC Act.

THEREFORE, IT IS ORDERED as follows:

FINDINGS

1. This Court has jurisdiction over this matter.
2. The Complaint charges that Defendant participated in deceptive and unfair acts or practices in violation of Section 5 of the FTC Act, 15 U.S.C. § 45, related to the privacy and security of video data collected by Defendant’s home security cameras.

3. Defendant neither admits nor denies any of the allegations in the Complaint, except as specifically stated in this Order. Only for purposes of this action, Defendant admits the facts necessary to establish jurisdiction.
4. Defendant waives any claim that it 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 agrees to bear its own costs and attorney fees.
5. Defendant and Plaintiff waive all rights to appeal or otherwise challenge or contest the validity of this Order.

DEFINITIONS

For purposes of this Order, the following definitions apply:

- A. **“Affected Work Product”** means any models or algorithms identified or reasonably identifiable by the Defendant as having been developed in whole or in part from review and annotation of Pre-March 2018 Covered Recordings.
- B. **“Affirmative Express Consent”** means any freely given, specific, informed, and unambiguous indication of an individual’s wishes demonstrating agreement by the individual, such as by a clear affirmative action, following a Clear and Conspicuous disclosure to the individual, apart from any privacy policy, terms of service, terms and conditions, or terms of use of all information material to the provision of such consent.

The following actions do not constitute Affirmative Express Consent:

1. Acceptance of general or broad terms of use or similar communication;
2. Hovering over, muting, pausing, or closing a given piece of content; or
3. Agreement obtained through a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice.

- C. **“Authorized User”** means the primary account holder associated with a Covered Home Security Product, and any user of a Covered Home Security Product authorized to access the account associated with the Covered Home Security Product by the primary account holder.
- D. **“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 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. On a product label, the disclosure must be presented on the principal display panel.

6. The disclosure must use diction and syntax understandable to ordinary consumers and must appear in each language in which the triggering representation appears.
 7. The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices and face-to-face communications.
 8. The disclosure must not be contradicted or mitigated by, or inconsistent with, anything else in the communication in which the disclosure is made.
 9. When the representation or sales practice targets a specific audience, such as children, the elderly, or the terminally ill, “ordinary consumers” includes ordinary members of that group.
- E. **“Covered Home Security Camera”** means any internet-enabled home security camera that Defendant designs, markets, and offers to consumers primarily for personal and residential use to record video.
- F. **“Covered Home Security Product”** means any Covered Home Security Camera and any related service that Defendant designs, markets, and offers to consumers to collect or store Covered Home Security Recordings (such as a subscription service or mobile application).
- G. **“Covered Home Security Recording”** means any pre-recorded or live-streaming audio, video, or photographic data collected by or on behalf of Defendant through a Covered Home Security Camera and, if such data is pre-recorded, stored by Defendant on behalf of the customer, except for audio, video, or photographic data (1) made publicly accessible on the internet, or made available to a party other than Defendant, by an Authorized User; or (2) submitted, with the Authorized User’s Affirmative Express Consent, to the Defendant for customer service, marketing, or research and development purposes.

- H. **“Covered Incident”** means any instance: (1) that results in Defendant notifying, pursuant to a statutory or regulatory requirement, any U.S. federal, state, or local government entity that Covered Home Security Recordings of or about an individual were, or are reasonably believed to have been, accessed, acquired, or publicly exposed without authorization; or (2) in which Defendant discovers that Covered Home Security Recordings of 10 or more Ring Accounts were, or are reasonably believed to have been, accessed, acquired, or publicly exposed without authorization. “Covered Incident” does not include any instance where the Covered Home Security Recordings were encrypted and the encryption key was not also accessed or acquired by an unauthorized person.
- I. **“Covered Information”** means the following information from or about an individual consumer that Defendant collects through a Covered Home Security Product, including any website or application that Defendant designs, markets, and offers to consumers: (1) authentication credential(s) sufficient to provide access to a user’s Ring Account, such as a user name and password; (2) a credit card, debit card, or financial institution account number; or (3) a Covered Home Security Recording.
- J. **“Face Embedding”** means data, such as a numeric vector, derived in whole or in part from an image of an individual’s face.
- K. **“Pre-March 2018 Covered Recordings”** means Covered Home Security Recordings collected before March 1, 2018 and reviewed and annotated by employees or contractors for research and development purposes.
- L. **“Defendant”** means Ring LLC (“Ring”) and its successors and assigns.

- M. **“Ring Account”** means any account provided by or on behalf of Defendant to any Authorized User through which an Authorized User may access any Covered Home Security Recording.
- N. **“Ring Principal Executive Officer”** means the individual serving as the Chief Executive Officer of Defendant, or such other officer (regardless of title) that is designated in Defendant’s bylaws or by resolution as having the duties of the principal executive officer of Defendant, acting solely in his or her official capacity on behalf of Defendant. In the event that such position is jointly held by two or more persons, then each of such persons shall be deemed to be a Ring Principal Executive Officer.

ORDER

I. PROHIBITION AGAINST MISREPRESENTATIONS ABOUT PRIVACY AND SECURITY

IT IS ORDERED that, for twenty years after entry of this Order, Defendant and Defendant’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 manufacturing, advertising, promotion, offering, sale, or distribution of any Covered Home Security Product, must not misrepresent in any manner, expressly or by implication:

- A. The extent to which, or the purposes for which, Defendant or any contractor working on Defendant’s behalf accesses, reviews, or discloses Covered Information; or
- B. The extent to which Defendant secures Covered Home Security Products against online attacks resulting from external actors’ misuse of valid authentication credentials of users of Covered Home Security Products.

II. MANDATED DELETION OF DATA AND AFFECTED WORK PRODUCT

IT IS FURTHER ORDERED that:

A. Defendant and Defendant'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 manufacturing, advertising, promotion, offering, sale, or distribution of any Covered Home Security Product, must, unless prohibited by law:

1. Within thirty (30) days of entry of this Order, delete or destroy all Pre-March 2018 Covered Recordings;
2. Within ninety (90) days of entry of this Order, delete or destroy all Face Embeddings collected before March 1, 2018 including through any Pre-March 2018 Covered Recordings; and
3. Within ninety (90) days of entry of this Order, delete or destroy any Affected Work Product unless such deletion is technically infeasible, in which case the Ring Principal Executive Officer must provide a written statement to the Commission within ninety (90) days of entry of this Order, sworn under penalty of perjury, identifying any such Affected Work Product, certifying that such deletion or destruction is technically infeasible, and providing a reasonable explanation for that determination. The written statement must be based on the personal knowledge of the Principal Executive Officer or subject matter experts upon whom the Principal Executive Officer reasonably relies in making the statement.

- B. Defendant must, within ninety (90) days of entry of this Order, provide a written statement to the Commission, sworn under penalty of perjury, confirming the deletion or destruction of all Covered Home Security Recordings, Face Embeddings, and Affected Work Product covered by Subprovision II.A above.

III. MANDATED PRIVACY AND DATA SECURITY PROGRAM

IT IS FURTHER ORDERED that Defendant must, within one hundred and eighty (180) days of entry of this Order, establish and implement, and thereafter maintain for twenty (20) years after entry of this Order, a comprehensive privacy and data security program (the “Program”) that protects the privacy, security, confidentiality, and integrity of Covered Information. To satisfy this requirement, Defendant must, at a minimum:

- A. Document in writing the relevant content, implementation, and maintenance of the Program;
- B. Provide the written program and any evaluations thereof or updates thereto to a senior officer responsible for the Program at least once every twelve (12) months and, in the event of a Covered Incident, within thirty (30) days after completion of response to the Covered Incident or sixty (60) days after the Covered Incident, whichever is sooner;
- C. Designate a qualified employee or employees to coordinate and be responsible for the Program;
- D. Assess and document, at least once every twelve (12) months and, in the event of a Covered Incident, within thirty (30) days after completion of a response to the Covered Incident or sixty (60) days after the Covered Incident, whichever is sooner, internal and external risks to the privacy, security, confidentiality, or integrity of

Covered Information (and, if conducted following a Covered Incident, related to the Covered Incident) that could result in the (1) unauthorized collection, maintenance, use, or disclosure of, or provision of access to, Covered Information; or the (2) misuse, loss, theft, alteration, destruction, or other compromise of such information;

- E. Design, implement, maintain, and document safeguards that control for the internal and external risks Defendant identifies to the privacy, security, confidentiality, or integrity of Covered Information identified in response to Subprovision III.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: (1) unauthorized collection, maintenance, use, or disclosure of, or provision of access to, Covered Information; or the (2) misuse, loss, theft, alteration, destruction, or other compromise of such information. Such safeguards must also include:
1. Not permitting any human review by Defendant's employees or contractors of any Covered Home Security Recording, unless, prior to such review, Defendant:
 - a) Implements a policy prohibiting such review unless it is:
 - (1) Required by law or legal process (such as a court order or search warrant);
 - (2) In connection with an investigation of suspected or actual illegal activity;
 - (3) To establish, exercise, or defend Defendant's legal rights;

- (4) Necessary or appropriate to prevent physical or other harm or financial loss; or
 - (5) Otherwise authorized by an Authorized User via Affirmative Express Consent; and
 - b) Requires any employee or contractor in a role that involves accessing Covered Home Security Recording(s) for such human review to attest that the reviewer will only access or view the Covered Home Security Recording for the purpose(s) specified by Defendant and for no other purpose; and
 - c) Requires that any such employees or contractors be trained on how to review Covered Home Security Recordings in accordance with the purpose specified by Defendant.
- 2. Periodically verifying, at least once every twelve (12) months, that the Defendant is restricting access to Covered Home Security Recordings as required by Subprovision III(E)(1);
- 3. Training of all employees and contractors whose responsibilities include access to Covered Information, at least every twelve (12) months, on how to safeguard Covered Information; provided, however, that this requirement shall not obligate Defendant to provide training to employees and contractors whose responsibilities only include access to encrypted Covered Information without the ability to decrypt them;

4. Data access controls for employee or contractor access to all databases and assets storing Covered Home Security Recordings, including by, at a minimum:
 - a) Restricting inbound connections to approved IP addresses or other equivalent or stronger protections;
 - b) Requiring multi-factor authentication methods for all employees, contractors, and affiliates in order to access any assets (including databases) storing Covered Home Security Recordings. Defendant may use equivalent industry authentication options that are not multi-factor, if the person responsible for the Program under Subprovision III.C: (1) approves in writing the use of such equivalent authentication options; and (2) documents a written explanation of how the authentication options are at least equivalent to the security provided by multi-factor authentication;
 - c) Limiting employee or contractor access to Covered Home Security Recordings to what is needed to perform that employee's or contractor's job function; and
 - d) Reviewing, at least once every twelve (12) months, employee and contractor access to Covered Home Security Recordings to ensure that the employee or contractor needs continued access to the Covered Home Security Recordings to perform the employee or contractor's job function; provided, however, that this requirement shall not obligate Defendant to implement data access controls for

employees and contractors who can only access encrypted Covered Home Security Recordings without the ability to decrypt them;

5. Technical measures to log and monitor employee and contractor access to Covered Information, including each instance in which a Covered Home Security Recording is accessed; provided, however, that this requirement shall not obligate Defendant to log and monitor access by employees and contractors to encrypted Covered Information without the ability to decrypt it;
6. Technical measures to secure Covered Home Security Products from online attacks resulting from the misuse of valid authentication credentials of users of Covered Home Security Products, such as:
 - a) Where passwords are used to secure users' Ring Accounts, requiring that users use strong passwords to secure their Ring Accounts, and recommending that they use unique passwords; and
 - b) Requiring multi-factor authentication methods be provided as an option for consumers to access Covered Home Security Recordings. Defendant may use equivalent industry authentication options that are not multi-factor, if the person responsible for the Program under Subprovision III.C: (1) approves in writing the use of such equivalent authentication options; and (2) documents a written explanation of how the authentication options are at least equivalent to the security provided by multi-factor authentication; and

7. Encryption in transit and at rest of all Covered Home Security Recordings in Defendant's control;
- F. Assess, at least once every twelve (12) months and, in the event of a Covered Incident, within thirty (30) days after completion of response to the Covered Incident or sixty (60) days after the Covered Incident, whichever is sooner, the sufficiency of any safeguards in place to address the internal and external risks to the privacy, security, confidentiality, or integrity of Covered Information (and, if conducted following a Covered Incident, related to the Covered Incident), and modify the Program as needed based on the results;
- G. Test and monitor the effectiveness of the safeguards at least once every twelve (12) months and, in the event of a Covered Incident, within thirty (30) days after completion of response to the Covered Incident or sixty (60) days after the Covered Incident, whichever is sooner (and, if conducted following a Covered Incident, related to the Covered Incident), and modify the Program as needed based on the results. Such testing and monitoring must include:
1. Vulnerability testing of Defendant's network(s) once every four (4) months and, in the event of a Covered Incident, within thirty (30) days after completion of response to the Covered Incident or sixty (60) days after the Covered Incident, whichever is sooner (and, if conducted following a Covered Incident, related to the Covered Incident);
 2. Vulnerability testing of the Covered Home Security Products before the launch of any new Covered Home Security Product or before any material change to any Covered Home Security Product, including any material

hardware or software update to the Covered Home Security Product and, in the event of a Covered Incident relating to a Covered Home Security Product, within thirty (30) days after completion of response to the Covered Incident or ninety (90) days after the Covered Incident, whichever is sooner; and

3. Penetration testing of Defendant's access controls described in Subprovision III.E(4) at least once every twelve (12) months and, in the event of a Covered Incident, within thirty (30) days after completion of response to the Covered Incident or sixty (60) days after the Covered Incident, whichever is sooner (and, if conducted following a Covered Incident, related to the Covered Incident);

H. Select and retain service providers capable of safeguarding Covered Information they access through or receive from Defendant, and contractually require such service providers to implement and maintain safeguards sufficient to address the internal and external risks to the privacy, security, confidentiality, or integrity of Covered Information; and

I. Evaluate and adjust the Program in light of any changes to Defendant's operations or business arrangements, a Covered Incident, new or more efficient technological or operational methods to control for the risks identified in Subprovision III.D of this Order, or any other circumstances that Defendant knows or has reason to know may have an impact on the effectiveness of the Program. At a minimum, Defendant must evaluate the Program at least once every twelve (12) months and modify the Program as needed based on the results.

IV. ASSESSMENTS BY A THIRD PARTY

IT IS FURTHER ORDERED that, in connection with its compliance with the Provision of this Order titled Mandated Privacy and Data Security Program, Defendant must obtain initial and biennial assessments (“Assessment(s)”):

- A. The Assessment must be obtained from one or more qualified, objective, independent third-party professionals (“Assessor(s)”) who: (1) use procedures and standards generally accepted in the profession; (2) conduct an independent review of the Program; (3) retain all documents relevant to each Assessment for five (5) years after completion of such Assessment; and (4) will provide such documents to the Commission within ten (10) days of receipt of a written request from a representative of the Commission. No documents may be withheld by the Assessor(s) on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney-client privilege, statutory exemption, or any similar claim. Defendant may obtain separate assessments for (1) privacy and (2) security, confidentiality, and integrity from multiple Assessors, so long as each of the Assessors meets the qualifications set forth above;
- B. For each Assessment, Defendant must provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission with the name(s), affiliation(s), and qualifications of the proposed Assessor(s), which the Associate Director shall have the authority to approve in her or his sole discretion;
- C. The reporting period for the Assessments must cover: (1) the first year after the entry date of the Order for the initial Assessment; and (2) each two-year period

thereafter for twenty (20) years after entry of the Order for the biennial Assessments;

D. Each Assessment must, for the entire assessment period:

1. Determine whether Defendant has implemented and maintained the Program required by Provision III of this Order titled Mandated Privacy and Data Security Program;
2. Assess the effectiveness of Defendant's implementation and maintenance of Subprovisions III.A-I;
3. Identify any gaps or weaknesses in, or instances of material noncompliance with, the Program;
4. Address the status of gaps or weaknesses in, or instances of material non-compliance with, the Program that were identified in any prior Assessment required by this Order; and
5. Identify specific evidence (including, but not limited to, documents reviewed, sampling and testing performed, and interviews conducted) examined to make such determinations, assessments, and identifications, and explain why the evidence that the Assessor examined is (a) appropriate for assessing an enterprise of the Defendant's size, complexity, and risk profile; and (b) sufficient to justify the Assessor's findings. No finding of any Assessment shall rely primarily on assertions or attestations by Defendant's management. The Assessment must be signed by the Assessor and must state that the Assessor conducted an independent review of the Program, and did not rely primarily on assertions or attestations by

Defendant's management, and state the number of hours that each member of the assessment team worked on the Assessment. To the extent that Defendant revises, updates, or adds one or more safeguards required under Subprovision III.E of this Order in the middle of an Assessment period, the Assessment must assess the effectiveness of the revised, updated, or added safeguard(s) for the time period in which it was in effect, and provide a separate statement detailing the basis for each revised, updated, or additional safeguard;

- E. Each Assessment must be completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Unless otherwise directed by a Commission representative in writing, Defendant must submit the initial Assessment to the Commission within ten (10) days after the Assessment has been completed via email to DEbrief@ftc.gov or 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, "FTC v. Ring LLC." All subsequent biennial Assessments must be retained by Defendant until the Order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request. The initial Assessment and any subsequent biennial Assessment provided to the Commission must be marked, in the upper right-hand corner of each page, with the words "DPIP Assessment" in red lettering.

V. COOPERATION WITH THIRD-PARTY ASSESSOR(S)

IT IS FURTHER ORDERED that Defendant, whether acting directly or indirectly, in connection with any Assessment required by Provision IV of this Order titled Assessments by a Third Party, must:

- A. Provide or otherwise make available to the Assessor all information and material in its possession, custody, or control that is relevant to the Assessment for which there is no reasonable claim of privilege or work product protection;
- B. Provide or otherwise make available to the Assessor information about Covered Home Security Products, Defendant's network(s), and all of Defendant's IT assets that is relevant to the Assessor's determination of the scope of the Assessment, and to provide visibility to those portions of the networks and IT assets deemed in scope; and
- C. Disclose all material facts to the Assessor(s), and not misrepresent in any manner, expressly or by implication, any fact material to the Assessor's: (1) determination of whether Defendant has implemented and maintained the Program required by Provision III of this Order titled Mandated Privacy and Data Security Program; (2) assessment of the effectiveness of the implementation and maintenance of Subprovisions III.A-I; or (3) identification of any gaps or weaknesses in, or instances of material non-compliance with, the Program.

VI. CERTIFICATIONS

IT IS FURTHER ORDERED that, one year after the entry date of this Order, and each year thereafter for twenty (20) years after the entry of this order:

- A. Defendant must provide the Commission with a certification from the Ring Principal Executive Officer that Defendant:
1. Has established, implemented, and maintained the requirements of this Order; and
 2. Is not aware of any material noncompliance with the requirements of this Order that has not been disclosed to the Commission.
 3. Each certification must be based on the personal knowledge of the Principal Executive Officer or subject matter experts upon whom the Principal Executive Officer reasonably relies in making the certification; and
- B. Unless otherwise directed by a Commission representative in writing, Defendant must submit all annual certifications to the Commission pursuant to this Order via email to DEbrief@ftc.gov or 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, “FTC v. Ring LLC.”

VII. COVERED INCIDENT REPORTS

IT IS FURTHER ORDERED that, for twenty (20) years after entry of this order, within a reasonable time after Defendant’s discovery of a Covered Incident, but in any event no later than ten (10) days after the Defendant first notifies any United States federal, state, or local entity of a Covered Incident or determines that no such notice is needed, the Defendant must submit a report to the Commission. The report must include, to the extent possible:

- A. The date, estimated date, or estimated date range when the Covered Incident occurred;

- B. A description of the facts relating to the Covered Incident, including the causes of the Covered Incident, if known;
- C. The number of consumers whose Covered Home Security Recordings were affected by the Covered Incident;
- D. The acts that Defendant has taken to date to remediate the Covered Incident and protect Covered Home Security Recordings from further exposure or access, and protect affected consumers from identity theft or other harm that may result from the Covered Incident; and
- E. A representative copy of any materially different notice sent by Defendant to consumers or to any U.S. federal, state, or local government entity.

Unless otherwise directed by a Commission representative in writing, all Covered Incident reports 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, “FTC v. Ring LLC.”

VIII. NOTICES TO CUSTOMERS

IT IS FURTHER ORDERED that Defendant must:

- A. Identify all consumers who had Ring accounts before February 1, 2018 (“eligible customers”). Ring must take reasonable efforts to identify such eligible customers, and their contact information. Eligible customers include those identified at any time;

- B. Notify all identified eligible customers by emailing each a notice in the form shown in Attachment A. The emailing of the notification letter must not include any other enclosures; and
- C. Notify all eligible customers within 180 days after the entry date of this Order and any eligible customers identified thereafter within 30 days of their identification.

IX. MONETARY JUDGMENT

IT IS FURTHER ORDERED that:

- A. Judgment in the amount of five million eight hundred thousand dollars (\$5,800,000) is entered in favor of the Commission against Defendant;
- B. Defendant is ordered to pay to the Commission five million eight hundred thousand dollars (\$5,800,000), which, as Defendant stipulates, their undersigned counsel holds in escrow for no purpose other than payment to the Commission; and
- C. Such payment must be made within seven (7) days of entry of this Order by electronic fund transfer in accordance with instructions previously provided by a representative of the Commission.

X. ADDITIONAL MONETARY PROVISIONS

IT IS FURTHER ORDERED that:

- A. Defendant relinquishes dominion and all legal and equitable right, title, and interest in all assets transferred pursuant to this Order and may not seek the return of any assets;
- B. The facts alleged in the Complaint will be taken as true, without further proof, in any subsequent civil litigation by or on behalf of the Commission to enforce its

rights to any payment or monetary judgment pursuant to this Order, such as a nondischargeability complaint in any bankruptcy case;

- C. The facts alleged in the Complaint establish all elements necessary to sustain an action by or on behalf of the Commission pursuant to Section 523(a)(2)(A) of the Bankruptcy Code, 11 U.S.C. § 523(a)(2)(A), and this Order will have collateral estoppel effect for such purposes;
- D. Defendant acknowledges that its Taxpayer Identification Numbers (Social Security Numbers or Employer Identification Numbers), which Defendant must submit, may be used for collecting and reporting on any delinquent amount arising out of this order, in accordance with 31 U.S.C. § 7701; and
- E. All money paid to the Commission pursuant to this Order may be deposited into a fund administered by the Commission or its designee to be used for equitable relief, including consumer redress and any attendant expenses for the administration of any redress fund. If a representative of the Commission decides that direct redress to consumers is wholly or partially impracticable or money remains after redress is completed, the Commission may apply any remaining money for such other equitable relief (including consumer information remedies) as it determines to be reasonably related to Defendant's practices alleged in the Complaint. Any money not used for such equitable relief is to be deposited to the U.S. Treasury as disgorgement. Defendant has no right to challenge any actions the Commission or its representatives may take pursuant to this Subprovision.

XI. CUSTOMER INFORMATION

IT IS FURTHER ORDERED that Defendant must directly or indirectly provide sufficient customer information to enable the Commission to efficiently administer consumer redress. If a representative of the Commission requests in writing any information related to redress, Defendant must provide it, in the form prescribed by the Commission, within fourteen (14) days.

XII. ACKNOWLEDGMENTS OF THE ORDER

IT IS FURTHER ORDERED that Defendant obtain acknowledgments of receipt of this Order:

- A. Defendant, within seven (7) of entry this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.
- B. For three (3) years after the entry date of this Order, Defendant must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members of Defendant; (2) all employees, agents, and representatives of Defendant managing 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 Reporting. Delivery must occur within seven (7) days of 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 Defendant delivered a copy of this Order, Defendant must obtain, within thirty (30) days, a signed and dated acknowledgment of receipt of this Order.

XIII. COMPLIANCE REPORTING

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

- A. One year after the entry date of this Order, Defendant must submit a compliance report, sworn under penalty of perjury:
 1. Defendant 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 Defendant; (b) identify all of Defendant's subsidiaries that collect, maintain, use, or disclose, or provide access to Covered Home Security Recordings by all of their names, telephone numbers, and physical, postal, email, and internet addresses; (c) describe the activities of each such subsidiary, including the goods and services offered, the means of advertising, marketing, and sales; (d) describe in detail whether and how Defendant is in compliance with each Provision of this Order; and (e) provide a copy of each Order Acknowledgment obtained pursuant to this Order, unless previously submitted to the Commission.
- B. For ten (10) years after entry of this Order, Defendant must submit a compliance notice, sworn under penalty of perjury, within fourteen (14) days of any change in:
 - (a) any designated point of contact; or
 - (b) the structure of Defendant that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary that engages in any acts or practices subject to this Order.

- C. Defendant must submit to the Commission notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against Defendant within fourteen (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: “FTC v. Ring LLC.”

XIV. RECORDKEEPING

IT IS FURTHER ORDERED that Defendant must create certain records for ten (10) years after the entry date of the Order, and retain each such record for five (5) years. Specifically, Defendant must create and retain the following records:

- A. accounting records showing the revenues from all goods or services sold relating to the subject matter of the Order, the costs incurred in generating those revenues, and resulting net profit or loss;

- B. personnel records showing, for each person who participates in conduct related to the subject matter of this Order, whether as an employee or otherwise, that person's name; job title or position; and dates of service;
- C. records of all consumer complaints and refund requests related to the subject matter of this Order received through Defendant's customer service channels, and any response, except to the extent that deletion of such records has been requested by a consumer;
- D. a copy of each unique advertisement or other marketing material making a representation subject to this Order;
- E. a copy of each widely externally-disseminated representation by Defendant that describes the extent to which, or the purposes for which, Defendant or any employee or contractor working on Defendant's behalf accesses or reviews any Covered Home Security Recording; and
- F. all records necessary to demonstrate full compliance with this Order, including all submissions to the Commission, all notices distributed pursuant to Provision VIII, and all documents related to Defendant's verifications pursuant to Subprovision III.E.2.

XV. COMPLIANCE MONITORING

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

- A. Within fourteen (14) days of receipt of a written request from a representative of the Commission, Defendant 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 Defendant. Defendant must permit representatives of the Commission to interview any employee or other person affiliated with Defendant who has agreed to such an interview. The person interviewed 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 Defendant or any individual or entity affiliated with Defendant, 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.

XVI. 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.

SO ORDERED this ____ day of ____, 2023.

United States District Judge

SO STIPULATED AND AGREED:

FOR PLAINTIFF

FEDERAL TRADE COMMISSION

/s/ Elisa Jillson

Elisa Jillson (DC Bar No. 989763)
Division of Privacy and Identity Protection
Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-3001 (voice); -3062 (fax)
Email: ejillson@ftc.gov

/s/ Andrew Hasty

Andrew Hasty (DC Bar No. 103398)
Division of Privacy and Identity Protection
Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-2861 (voice); -3062 (fax)
Email: ahasty@ftc.gov

/s/ Miles Plant

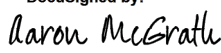
Miles Plant (NY Bar No. 4901583)
Division of Privacy and Identity Protection
Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-2861 (voice); -3062 (fax)
Email: mplant@ftc.gov

/s/ Julia Horwitz

Julia Horwitz (DC Bar No. 1018561)
Division of Privacy and Identity Protection
Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-2269 (voice); -3062 (fax)
Email: jhorwitz@ftc.gov

FOR DEFENDANT:

RING LLC

DocuSigned by:


Aaron McGrath
Authorized Signatory for Ring LLC

Date: May 24, 2023

DocuSigned by:


Laura Kim (DC Bar No. 473143)*
Caleb Skeath (DC Bar No. 1030678)*
Nikhil Singhvi (DC Bar No. 496357)
Covington & Burling LLP
One CityCenter, 850 Tenth Street, NW
Washington, DC 20001-4956
(202) 662-5333 (Kim)
(202) 662-5119 (Skeath)
(202) 662-5306 (Singhvi)
Email: lkim@cov.com
Email: cskeath@cov.com
Email: nsinghvi@cov.com

Date: May 24, 2023

Alexandra Scott (CA Bar No. 320012)*
Covington & Burling LLP
3000 El Camino Real, 5 Palo Alto Square, 10th Floor
(650) 632-4743
Email: ajscott@cov.com

Attorneys for Defendant
*Pro hac vice motion pending

ATTACHMENT A

Attachment A

[Ring Letterhead]

Dear Neighbor:

On [date], we entered into a settlement with the Federal Trade Commission – the nation’s consumer protection agency – to resolve the FTC’s allegations that more employees and contractors than necessary had access to the stored videos collected by Ring cameras. The FTC alleges that several years ago, a limited number of employees viewed customers’ videos without their permission and without a business reason. These individuals are no longer employed by Ring.

Since 2018, we have significantly changed our access and review practices. Now, only a very small number of employees can access videos, and only in very limited circumstances. You can learn more about our privacy practices at [XXX].

Visit [XXX] for more information about this settlement.