UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Joseph J. Simons, Chairman**
Noah Joshua Phillips
Rohit Chopra
Rebecca Kelly Slaughter
Christine S. Wilson

In the Matter of **ZOOM VIDEO COMMUNICATIONS, INC., a corporation, d/b/a ZOOM.**	**FILE No. 192 3167** **AGREEMENT CONTAINING CONSENT ORDER**

The Federal Trade Commission ("Commission") has conducted an investigation of certain acts and practices of Zoom Video Communications, Inc. ("Proposed Respondent"). The Commission's Bureau of Consumer Protection ("BCP") has prepared a draft of an administrative Complaint ("draft Complaint"). BCP and Proposed Respondent, through its duly authorized officer, enter into this Agreement Containing Consent Order ("Consent Agreement") to resolve the allegations in the attached draft Complaint through a proposed Decision and Order to present to the Commission, which is also attached and made a part of this Consent Agreement.

IT IS HEREBY AGREED by and between Proposed Respondent and BCP, that:

1. The Proposed Respondent is Zoom Video Communications, Inc., also doing business as Zoom, a Delaware Corporation with its principal office or place of business at 55 Almaden Boulevard, 6th Floor, San Jose, California, 95113.

2. Proposed Respondent neither admits nor denies any of the allegations in the Complaint, except as specifically stated in the Decision and Order. Only for purposes of this action, Proposed Respondent admits the facts necessary to establish jurisdiction.

3. Proposed Respondent waives:

   a. Any further procedural steps;

   b. The requirement that the Commission's Decision contain a statement of findings of fact and conclusions of law; and

   c. All rights to seek judicial review or otherwise to challenge or contest the validity of the Decision and Order issued pursuant to this Consent Agreement.

4. This Consent Agreement will not become part of the public record of the proceeding unless and until it is accepted by the Commission. If the Commission accepts this Consent Agreement, it, together with the draft Complaint, will be placed on the public record for 30 days and information about them publicly released. Acceptance does not constitute final approval, but it serves as the basis for further actions leading to final disposition of the matter. Thereafter, the Commission may either withdraw its acceptance of this Consent Agreement and so notify Proposed Respondent, in which event the Commission will take such action as it may consider appropriate, or issue and serve its Complaint (in such form as the circumstances may require) and decision in disposition of the proceeding, which may include an Order. *See* Section 2.34 of the Commission's Rules, 16 C.F.R. § 2.34 ("Rule 2.34").

5. If this agreement is accepted by the Commission, and if such acceptance is not subsequently withdrawn by the Commission pursuant to Rule 2.34, the Commission may, without further notice to Proposed Respondent: (1) issue its Complaint corresponding in form and substance with the attached draft Complaint and its Decision and Order; and (2) make information about them public. Proposed Respondent agrees that service of the Order may be effected by its publication on the Commission's website (ftc.gov), at which time the Order will become final. *See* Rule 2.32(d). Proposed Respondent waives any rights it may have to any other manner of service. *See* Rule 4.4.

6. When final, the Decision and Order will have the same force and effect and may be altered, modified, or set aside in the same manner and within the same time provided by statute for other Commission orders.

7. The Complaint may be used in construing the terms of the Decision and Order. No agreement, understanding, representation, or interpretation not contained in the Decision and Order or in this Consent Agreement may be used to vary or contradict the terms of the Decision and Order.

8. Proposed Respondent agrees to comply with the terms of the proposed Decision and Order from the date that Proposed Respondent signs this Consent Agreement. Proposed Respondent understands that it may be liable for civil penalties and other relief for each violation of the Decision and Order after it becomes final.

ZOOM VIDEO COMMUNICATIONS, INC.

By:_____
Eric Yuan
Chief Executive Officer

Date:_____

By:_____
Travis LeBlanc, Esq.
Cooley LLP
Attorney for Proposed Respondent

Date:_____

FEDERAL TRADE COMMISSION

By:_____
Linda Holleran Kopp
Attorney, Bureau of Consumer Protection

By:_____
Ryan Mehm
Attorney, Bureau of Consumer Protection

By:_____
Caroline Schmitz
Attorney, Bureau of Consumer Protection

APPROVED:

By: _____
Maneesha Mithal
Associate Director, Division of Privacy & Identity Protection

By: _____
Andrew Smith
Director, Bureau of Consumer Protection

Date:_____

192 3167

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Joseph J. Simons, Chairman**
Noah Joshua Phillips
Rohit Chopra
Rebecca Kelly Slaughter
Christine S. Wilson

In the Matter of **ZOOM VIDEO COMMUNICATIONS, INC., a corporation, d/b/a ZOOM.**	**DECISION AND ORDER** **DOCKET NO. C-**

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 Zoom Video Communications, Inc., a Delaware corporation, with its principal office or place of business at 55 Almaden Boulevard, 6th Floor, San Jose, California 95113.

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

ORDER

Definitions

For purposes of this Order, the following definitions apply:

A. "**Covered Incident**" means any instance in which any United States federal, state, or local law or regulation ("Breach Notification Law") requires, or would require if recorded or livestream video or audio content from a Meeting were included as a type of personal information covered by such Breach Notification Law, Respondent to notify any U.S. federal, state, or local government entity that information collected or received, directly or indirectly, by Respondent from or about an individual consumer was, or is reasonably believed to have been, accessed or acquired without authorization. For purposes of this definition, "Covered Incident" does not include any instance of unauthorized access or acquisition of video or audio content if Respondent determines that such instance: (a) affected fewer than 500 Users; (b) resulted from a User accessing the video or audio content by using a link, password, or other access information, obtained directly or indirectly, as a result of its distribution by a Meeting host or organizer; or (c) resulted from a Meeting that is offered or made publicly accessible by the Meeting host or organizer; or (d) the video or audio content was encrypted and the encryption key was not also accessed or acquired from Respondent by an unauthorized person.

B. "**Covered Information**" means information from or about an individual, including: (a) a first and last name; (b) a physical address; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a telephone number; (e) a Social Security number; (f) a driver's license or other government-issued identification number; (g) a financial institution account number; (h) credit or debit card information; (i) recorded or livestream video or audio content, chat transcripts, documents, or any other multimedia content shared by Users during a Meeting; (j) 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 (k) any information combined with any of (a) through (j) above.

C. "**Credential**" or "**Credentials**" means the user name and password that a User utilizes for logging in or otherwise accessing Respondent's products or services.

D. "**Meeting**" means a one-on-one or group videoconference on Respondent's platform, including but not limited to, webinars and conference room videoconference connectors.

E. "**Meeting Service**" **or** "**Meeting Services**" means all features and ancillary services developed by or on behalf of Respondent and used in the context of a Meeting (*e.g.*, video, audio, chat, content-sharing, recording, and storage of recordings). "Meeting Service" or "Meeting Services" does not include any plugin, cookie, or application that is offered or provided by a third party, including but not limited to, applications offered by third parties through the Zoom app store.

F. "**Respondent**" or "**Zoom**" means Zoom Video Communications, Inc., and its successors and assigns.

G. "**Third-Party Security Feature**" means any feature or tool built into an internet browser or operating system that: (a) has been specified as a security feature in the developer's official release notes; or that (b) has been identified by Zoom Security Personnel designated by Respondent for this purpose, based on their experience and expertise in secure software development principles, as a feature that protects the security of a User against the risk of unauthorized access, collection, disclosure, use, misuse, loss, theft, alteration, destruction, or other compromise of the User's Covered Information. "Third-Party Security Feature" does not include any software, system, feature, or tool, including without limitation, any plugin, cookie, or application, that is not developed by or for the browser or operating system developer.

H. "**User**" means any entity or individual that uses Zoom's Meeting Services.

I. "**Zoom Security Personnel**" means any person(s) working by or on behalf of Respondent who has been trained in secure software development principles, including secure engineering and defensive programming concepts, such as Respondent's Chief Information Security Officer.

Provisions

I. Prohibited 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 any product or service, must not misrepresent in any manner, expressly or by implication:

A. Respondent's collection, maintenance, use, deletion, or disclosure of any Covered Information;

B. The security features, or any feature that impacts a Third-Party Security Feature, included in any Meeting Service, or the material changes included in any updates thereof;

C. The extent to which Respondent protects any Covered Information from unauthorized access;

D. The extent to which a User can control the privacy or security of any Covered Information collected and maintained by Respondent, and the steps the User must take to implement such controls;

E. The categories of third parties to which Respondent makes Covered Information accessible; or

F. The extent to which Respondent otherwise maintains the privacy, security, confidentiality, or integrity of Covered Information.

II. Mandated Information Security Program

IT IS FURTHER ORDERED that Respondent, and 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, within sixty (60) days of issuance of this order, establish and implement, and thereafter maintain, a comprehensive information security program ("Program" or "Information Security Program") that protects the security, confidentiality, and integrity of such Covered Information. To satisfy this requirement, Respondent must, at a minimum:

A. Document in writing the content, implementation, and maintenance of the Program, including all processes and procedures that will be used to implement all Program policies and safeguards;

B. Provide the written Program and any material evaluations thereof or material updates thereto to Respondent's board of directors or governing body or, if no such board or equivalent governing body exists, to a senior officer of Respondent responsible for Respondent's Program at least once every twelve (12) months and promptly (not to exceed thirty (30) days) after a Covered Incident;

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 promptly (not to exceed thirty (30) days) following a Covered Incident, internal and external risks to the security, confidentiality, or integrity of Covered Information 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 Respondent identifies to the security, confidentiality, and integrity of Covered Information identified in response to sub-Provision II.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. Implementing a security review by Zoom Security Personnel designated by Respondent of all new Meeting Services software or software updates, prior to release that, at a minimum, includes:

    a. Policies, procedures, and any applicable technical measures for reviewing all new Meeting Service software or software updates for commonly known vulnerabilities, including those identified by the Open Web Application Security Project (OWASP) and critical or high severity vulnerabilities in the National Vulnerability Database (NVD), and remediating or otherwise mitigating any such vulnerabilities;

    b. Policies, procedures, and any applicable technical measures to: (i) determine whether any new Meeting Services software or software update is designed to circumvent or bypass, in whole or in part, any Third-Party Security Feature such that the Third-Party Security Feature no longer provides the same protection(s) for Users against the risk of unauthorized access, collection, disclosure, use, misuse, loss, theft, alteration, destruction, or other compromise of Users' Covered Information; and (ii) assess the risk of unauthorized access, collection, disclosure, use, misuse, loss, theft, alteration, destruction, or other compromise of the User's Covered Information that will result from such circumvention or bypass, based on the volume and sensitivity of Covered Information that is at risk, and the likelihood that the risk could be realized; and

    c. Policies, procedures, and any applicable technical measures so that Respondent will not implement any new Meeting Services software or software update that has been identified under Part II.E.1.b(i) of this Order as designed to circumvent or bypass a Third-Party Security Feature, unless: (i) Zoom Security Personnel determine that the bypass or circumvention does not create a material risk of unauthorized access, collection, disclosure, use, misuse, loss, theft, alteration, destruction, or other compromise of Users' Covered Information; or (ii) Respondent implements security measure(s) that offset or otherwise mitigate the risk(s) of unauthorized access, collection, disclosure, use, misuse, loss, theft, alteration, destruction, or other compromise of Users' Covered Information that were identified under Part II.E.1.b(ii) of this Order;

2. Implementing a vulnerability management program that includes:

    a. Conducting vulnerability scans of Respondent's networks and systems on at least a quarterly basis; and

b. Policies, procedures, and any applicable technical measures for remediating or otherwise mitigating any critical or high severity vulnerabilities promptly (but in no event later than thirty (30) days after the vulnerability is detected), unless Respondent documents its rationale for not doing so;

3. Implementing a default, randomized naming convention for recorded Meetings that are to be stored on Users' local devices, and instructing Users to employ a unique file name when saving such recorded Meetings;

4. Policies, procedures, and any applicable technical measures to: (a) systematically classify and inventory Covered Information in Respondent's control; (b) log and monitor access to repositories of Covered Information in Respondent's control; and (c) limit access to Covered Information by, at a minimum, limiting employee and service provider access to Covered Information to what is needed to perform that employee or service provider's job function;

5. Data deletion policies, procedures, and any applicable technical measures, including validating that all copies of Covered Information identified for deletion are deleted within thirty-one (31) days;

6. Policies, procedures, and any applicable technical measures designed to reduce the risk of online attacks resulting from the misuse of valid Credentials by unauthorized third parties, including: (a) requiring Users to secure their accounts with strong, unique passwords; (b) using automated tools to identify non-human login attempts; (c) rate-limiting login attempts to minimize the risk of a brute force attack; and (d) implementing password resets for known compromised Credentials;

7. Regular security training programs, on at least an annual basis, that are updated, as applicable, to address internal or external risks identified by Respondent under sub-Provision II.D of this Order, and that include, at a minimum:

   a. Security awareness training for all employees on Respondent's security policies and procedures, including the requirements of this Order and the process for submitting complaints and concerns; and

   b. Training in secure software development principles, including secure engineering and defensive programming concepts, for developers, engineers, and other employees that design Respondent's products or services or that are otherwise responsible for the security of Covered Information;

8. Technical measures to monitor all of Respondent's networks, systems, and assets within those networks to identify anomalous activity and/or data security events on Respondent's network, including unauthorized attempts to exfiltrate Covered Information from Respondent's networks;

9. Incident response policies, procedures, and any applicable technical measures, including centralized log management and documenting remedial security actions;

10. Technical measures designed to safeguard against unauthorized access to any network or system that stores, collects, maintains, or processes Covered Information, such as properly configured firewalls; properly configured physical or logical segmentation of networks, systems, and databases; and securing of remote access to Respondent's networks through multi-factor authentication or similar technology except for when accessing such networks is for the purpose of using Meeting Services; and

11. Protections, such as encryption, tokenization, or other same or greater protections, for Covered Information collected, maintained, processed, or stored by Respondent, including in transit and at rest;

F. Assess, at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following a Covered Incident, the sufficiency of any safeguards in place to address the internal and external risks to the security, confidentiality, and integrity of Covered Information, and modify the Program based on the results;

G. Test and monitor the effectiveness of the safeguards at least once every twelve (12) months and promptly (not to exceed thirty (30) days) following a Covered Incident, and modify the Program based on the results. Such testing and monitoring must include penetration testing of Respondent's network at least once every twelve (12) months and promptly (not to exceed thirty (30) days) after a Covered Incident;

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

I. Consult with, and seek appropriate guidance from, independent, third-party experts on data protection in the course of establishing, implementing, maintaining, and updating the Program; and

J. Evaluate and adjust the Program in light of any changes to Respondent's operations or business arrangements, a Covered Incident, new or more efficient technological or operational methods to control for the risks identified in sub-Provision II.D of this Order, or any other circumstances that Respondent knows or has reason to know may have a material 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 twelve (12) months and modify the Program as necessary based on the results.

III. Independent Program Assessments by a Third Party

IT IS FURTHER ORDERED that, in connection with compliance with Provision II of this Order, titled Mandated Information Security Program, Respondent must obtain initial and biennial assessments ("Assessments"):

A. The Assessments must be obtained from one or more qualified, objective, independent third-party professionals ("Assessor"), who: (1) uses procedures and standards generally accepted in the profession; (2) conducts an independent review of the Program; and (3) retains 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 on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney-client privilege, statutory exemption, or any similar claim;

B. For each Assessment, Respondent must provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission with the name(s), affiliation, and qualifications of the proposed Assessor, whom 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 one hundred eighty (180) days after the Information Security Program has been put in place for the initial Assessment; and (2) each two-year period thereafter for twenty (20) years after issuance of the Order for the biennial Assessments;

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

1. Determine whether Respondent has implemented and maintained the Information Security Program required by Provision II of this Order, titled Mandated Information Security Program;

2. Assess the effectiveness of Respondent's implementation and maintenance of sub-Provisions II.A-J;

3. Identify any gaps or weaknesses in, or instances of material noncompliance with, the Information Security Program;

4. Address the status of gaps or weaknesses in, or instances of material non-compliance with, the Information Security Program that were identified in any prior Assessment required by this Order; and

5. Identify specific evidence (including 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 Respondent'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 Respondent's management. The Assessment must be signed by the Assessor, state that the Assessor conducted an independent review of the Information Security Program and did not rely primarily on assertions or attestations by Respondent's

management, and state the number of hours that each member of the assessment team worked on the Assessment. To the extent that Respondent revises, updates, or adds one or more safeguards required under Provision II of this Order during 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; and

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, Respondent 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, "In re Zoom Video Communications, Inc., FTC File No. 192 3167." All subsequent biennial Assessments must be retained by Respondent until the order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request.

IV. Cooperation with Third Party Assessor(s)

IT IS FURTHER ORDERED that Respondent, whether acting directly or indirectly, in connection with any Assessment required by Provision III of this Order, titled Independent Program 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;

B. Provide or otherwise make available to the Assessor information about Respondent's networks and all of Respondent's IT assets so that the Assessor can determine the scope of the Assessment, and visibility to those portions of the networks and IT assets deemed in scope; and

C. Disclose all material facts to the Assessor, and not misrepresent in any manner, expressly or by implication, any fact material to the Assessor's: (1) determination of whether Respondent has implemented and maintained the Information Security Program required by Provision II of this Order, titled Mandated Information Security Program; (2) assessment of the effectiveness of the implementation and maintenance of sub-Provisions II.A-J; or (3) identification of any gaps or weaknesses in, or instances of material noncompliance with, the Information Security Program.

V. Annual Certification

IT IS FURTHER ORDERED that Respondent must:

A. One (1) year after the issuance date of this Order, and each year thereafter, provide the Commission with a certification from a senior corporate manager, or, if no such senior corporate manager exists, a senior officer of Respondent responsible for Respondent's Information Security Program that: (1) Respondent has established, implemented, and maintained the requirements of this Order; and (2) Respondent is not aware of any material noncompliance that has not been (a) corrected or (b) disclosed to the Commission. The certification must be based on the personal knowledge of the senior corporate manager, senior officer, or subject matter experts upon whom the senior corporate manager or senior officer reasonably relies in making the certification.

B. Unless otherwise directed by a Commission representative in writing, 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: "In re Zoom Video Communications, Inc., FTC File No. 192 3167."

VI. Covered Incident Reports

IT IS FURTHER ORDERED that Respondent, within thirty (30) days after the date of Respondent's discovery of a Covered Incident, but in any event no later than ten (10) days after the date Respondent first notifies any U.S. federal, state, or local government entity of the Covered Incident, 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. A description of each type of Covered Information that was affected or triggered any notification obligation to the U.S. federal, state, or local government entity;

D. The number of consumers whose information was affected or that triggered the notification obligation to the U.S. federal, state, or local government entity;

E. The acts that Respondent has taken to date to remediate the Covered Incident and protect Covered Information from further exposure or access, and protect affected individuals from identity theft or other harm that may result from the Covered Incident; and

F. A representative copy of any materially different notice sent by Respondent 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: "In re Zoom Video Communications, Inc., FTC File No. 192 3167."

VII. Acknowledgments of the Order

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

A. Respondent, within ten (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 five (5) years after the issuance date of this Order, Respondent must deliver a copy of this Order to: (a) all principals, officers, directors, and LLC managers and members; (b) all employees, agents, and representatives with managerial responsibilities related to the subject matter of the Order; and (c) any business entity resulting from any change in structure as set forth in the Provision titled Compliance Reports and Notices. Delivery must occur within ten (10) days after the effective date of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities; and

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.

VIII. Compliance Reports and Notices

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

A. One (1) 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, and the means of collection, maintenance, use, deletion, or disclosure of information; (d) describe in detail whether and how Respondent is in compliance with each Provision of this Order; and (e) provide a copy of each Acknowledgment of the Order obtained pursuant to this Order, unless previously submitted to the Commission;

B. Respondent must submit a compliance notice, sworn under penalty of perjury, within fourteen (14) days of any change in the following: (a) any designated point of contact; or (b) the structure of the 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 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; and

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 Zoom Video Communications, Inc., FTC File No. 192 3167."

IX. Recordkeeping

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

A. Accounting records showing the revenues from all goods or services sold;

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 U.S. consumer complaints that were submitted to Respondent and relate to the subject matter of the Order, and any response(s) to such complaints;

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

E. A copy of each widely disseminated and materially different representation by Respondent that describes (a) Respondent's collection, maintenance, use, deletion, or disclosure of any Covered Information; (b) the security features, or any features that impact a Third-Party Security Feature, included in any Meeting Service, or the changes included in any updates thereof; (c) the extent to which Respondent protects Covered Information from unauthorized access, including any representation on any website or other service controlled by Respondent that relates to the privacy, security,

confidentiality, and integrity of Covered Information; (d) the extent to which a User can control the privacy or security of Covered Information and the steps the User must take to implement such controls; and (e) the categories of third parties to which Respondent makes Covered Information accessible; and

F. For five (5) years after the date of preparation of each Assessment required by this Order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of Respondent, including all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials concerning Respondent's compliance with related Provisions of this Order, for the compliance period covered by such Assessment.

X. Compliance Monitoring

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

A. Within fourteen (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, appear for depositions, 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; and

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.

XI. 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 twenty (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 twenty (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 twenty (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.

April J. Tabor
Acting Secretary

SEAL:
ISSUED: