Analysis of Proposed Consent Order to Aid Public Comment
***In the Matter of Zoom Video Communications, Inc.*, File No. 192 3167**

The Federal Trade Commission ("Commission") has accepted, subject to final approval, an agreement containing a consent order from Zoom Video Communications, Inc. ("Zoom").

The proposed consent order ("proposed order") has been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission will again review the agreement and the comments received, and will decide whether it should withdraw from the agreement and take appropriate action or make final the agreement's proposed order.

This matter involves Zoom, a videoconferencing platform provider that provides customers with videoconferencing services and various add-on services, such as cloud storage. Zoom's core product is the Zoom "Meeting," which is a platform for one-on-one and group videoconferences. Users can also, among other things, chat with others in the Meeting, share their screen, and record videoconferences.

In its proposed five-count complaint, the Commission alleges that Zoom violated Section 5(a) of the Federal Trade Commission Act. First, the proposed complaint alleges that Zoom misrepresented to users since at least June 2016 that they could secure all Meetings with end-to-end encryption. End-to-end encryption is a method of securing communications where an encrypted communication can only be deciphered by the communicating parties. No other person—not even the platform provider—can decrypt the communication because they do not possess the necessary cryptographic keys to do so. Contrary to its representations to users, Zoom did not provide end-to-end encryption for all Meetings because Zoom's servers maintained the cryptographic keys that could allow Zoom to access the content of its customers' Meetings.

Second, the proposed complaint alleges that Zoom misrepresented the level of encryption it used to secure communications between participants using Zoom's video conferencing service. Specifically, Zoom had claimed since at least June 2016 that it secured Meetings, in part, with Advanced Encryption Standard (AES) and using a 256-bit encryption key ("AES 256-bit encryption"). The 256-bit encryption key refers to the length of the key needed to decrypt the communication. Generally speaking, a longer encryption key provides more confidentiality protection than shorter keys because there are more possible key combinations, thereby making it harder to find the correct key and crack the encryption. Contrary to its representation to users, Zoom in fact secured its Meetings with AES with a 128-bit encryption key.

Third, the proposed complaint alleges that Zoom misrepresented that, for users who opted to store recordings of their Zoom Meetings in Zoom's secure cloud storage ("Cloud Recordings"), Zoom would process and store such recordings in Zoom's cloud "once the meeting has ended." Contrary to its representations to users, Zoom kept Cloud Recordings on Zoom's servers for up to 60 days, unencrypted, before transferring them to Zoom's secure cloud storage, where they are then stored encrypted.

Fourth, the proposed complaint alleges that Zoom violated Section 5 when it installed a local hosted web server (called "ZoomOpener") on 3.8 million users' Mac computers. In July

2018, Zoom updated its application for Mac desktop computers by secretly deploying a web server onto users' computers. The ZoomOpener web server was designed to circumvent a security and privacy safeguard in Apple's Safari browser. Apple had updated its Safari browser to help defend its users from malicious actors and popular malware by requiring interaction with a dialogue box when a website or link attempts to launch an outside App. As a result of the new browser safeguard, users who clicked on a link to join a Zoom Meeting would receive an additional prompt that read, "Do you want to allow this page to open 'zoom.us'?" If the user selected "Allow," the browser would connect the user to the Meeting, while clicking "Cancel" would end the interaction and prevent the Zoom application from launching. The ZoomOpener web server was designed to avoid this extra prompt. It also remained on users' computers even after users deleted the Zoom application, and would automatically reinstall the Zoom app—without any user interaction—if the user clicked on a link to join a Zoom Meeting or visited a website that had a Zoom Meeting embedded in it.

The proposed complaint alleges that it was an unfair act or practice for Zoom, without adequate notice or consent, to circumvent the Safari browser safeguard without implementing any measures to compensate for the circumvented privacy and security protections. The proposed complaint alleges that doing so caused or was likely to cause substantial injury to consumers, that consumers could not reasonably avoid themselves, and that was not outweighed by countervailing benefits to consumers or competition. Apple removed the ZoomOpener web server from users' computers through an automatic update in July 2019.

And finally, the proposed complaint alleges that Zoom violated Section 5 when it represented that it was updating its Mac application in order to resolve minor bug fixes, but failed to disclose, or failed to disclose adequately, the material information that the update would deploy the ZoomOpener web server, that the web server would circumvent a Safari browser privacy and security safeguard, or that the web server would remain on users' computers even after they had uninstalled Zoom's Mac application.

Part I of the proposed order prohibits Zoom from misrepresenting its privacy and security practices in the future. It prohibits, for example, misrepresentations about Zoom's collection, maintenance, use, deletion, or disclosure of Covered Information; the security features, or any feature that impacts a third-party security feature, included in any Meeting Service; or the extent to which Respondent otherwise maintains the privacy, security, confidentiality, or integrity of Covered Information. "Covered Information" means information from or about an individual.

Part II of the proposed order requires Zoom to establish, implement, and maintain a comprehensive information security program that protects the security, confidentiality, and integrity of Covered Information. Among other things, Zoom must implement specific security safeguards, such as a security review for all new software, a vulnerability management program for its internal networks, security training for its employees, inventorying personal information stored in its systems and implementing data deletion policies, and other specific security measures, such as proper network segmentation and remote access authentication.

Part III of the proposed order requires Zoom to obtain initial and biennial data security assessments for twenty years.

Part IV of the agreement requires Zoom to disclose all material facts to the assessor and prohibits Respondent from misrepresenting any fact material to the assessments required by Part III.

Part V requires Zoom to submit an annual certification from a senior corporate manager (or senior officer responsible for its information security program) that it has implemented the requirements of the Order, and is not aware of any material noncompliance that has not been corrected or disclosed to the Commission.

Part VI requires Zoom to submit a report to the Commission of its discovery of any Covered Incident. A "Covered Incident" is when any federal, state, or local law or regulation requires Zoom to notify any federal, state, or local government entity that information collected or received by Zoom from or about an individual consumer was, or is reasonably believed to have been, accessed or acquired without authorization. Video and audio content are specifically included as a type of personal information that would trigger notification.

Parts VII through X of the proposed order are reporting and compliance provisions. Part VII requires acknowledgement of the order and dissemination of the order now and in the future to persons with responsibilities relating to the subject matter of the order. Part VIII ensures notification to the FTC of changes in corporate status and mandates that the company submit an initial compliance report to the FTC. Part IX requires the company to create and retain certain documents relating to its compliance with the order. Part X mandates that the company make available to the FTC information or subsequent compliance reports, as requested.

Part XI states that the proposed order will remain in effect for 20 years, with certain exceptions.

The purpose of this analysis is to aid public comment on the proposed order. It is not intended to constitute an official interpretation of the complaint or proposed order, or to modify in any way the proposed order's terms.