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 MeetinTiiAdvanced Encryption Standard (AES) and used a 256-bit encryption key “AES 256-bit encryption” (g ti0 (’y e)–4TJ(i)2-1ike)-2-16 (T d)]TJ k20 (0 Tu)].21 02 0 Tpr)-4 (4)]TJ 0 Tu)]TJ e

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 reins

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