

Complaint

IN THE MATTER OF

ZOOM VIDEO COMMUNICATIONS, INC.**D/B/A****ZOOM**CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF SECTION 5 OF THE FEDERAL
TRADE COMMISSION ACT*Docket No. C-4731; File No. 192 3167**Complaint, January 19, 2021 – Decision, January 19, 2021*

This consent order addresses Zoom Video Communications, Inc.’s representations regarding their videoconferencing services and various add-on services, such as cloud storage. The complaint alleges that Zoom violated Section 5(a) of the Federal Trade Commission Act by representing that consumers could secure all Meetings with end-to-end encryption using, in part, Advanced Encryption Standard (AES) and a 256-bit encryption key; and that recorded meetings would be stored in their secure cloud storage “once the meeting has ended.” The complaint further alleges that Zoom 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, which would circumvent a Safari browser privacy and security safeguard, and would remain on users’ computers even after they had uninstalled Zoom’s Mac application. The consent order prohibits Zoom from misrepresenting its privacy and security practices in the future.

Participants

For the *Commission*: Linda Holleran Kopp, Ryan Mehm, and Caroline Schmitz.

For the *Respondents*: Dee Bansal, Scott Dailard, David Houska, Jina John, Travis LeBlanc, Kaitland Kennelly, David Mills, and David Navetta, Cooley LLP.

COMPLAINT

The Federal Trade Commission, having reason to believe that Zoom Video Communications, Inc., a corporation (“Respondent”), has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

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

2. The acts and practices of Respondent Zoom alleged in this complaint have been in or affecting commerce, as “commerce” is defined in Section 4 of the Federal Trade Commission Act.

Complaint

Respondent's Business Practices

3. Founded in 2011, Zoom is a videoconferencing platform provider that provides customers with videoconferencing services and various add-on services, such as cloud storage. Zoom's 2019 annual revenue was \$622.7 million; its Q1 2020 revenue was \$328.2 million. Zoom has over 2,000 employees.

4. Zoom's core product is the Zoom "Meeting," which is a platform for one-on-one and group videoconferences. Zoom Meetings also have the capability, among other things, for accompanying chat messages, screen sharing, and the recording of videoconferences. Zoom offers certain customers the option to host Zoom's videoconferencing services on the customer's internal network through its "Connector" product.

5. A Zoom Meeting is comprised of a host who organizes the Meeting and the individual attendees who participate in those video meetings. To schedule and host a Zoom Meeting, a user must create a Zoom account and download Zoom's software application ("Zoom App") for desktop or laptop (e.g., Windows or Mac) or mobile (e.g., iOS or Android).

6. By creating a Zoom account, a user can create and host a videoconference and invite others to attend by providing them with a hyperlink, conference identifier, or telephone dial-in instructions. To join a Meeting, individual attendees typically download the Zoom App, but do not need to create a Zoom account. Rather than download the Zoom App, attendees can also join a Meeting through their browser or by telephone. Attendees who join a Meeting through their browser or by telephone do not have access to all of the same features that are available through the Zoom App.

7. Zoom offers its videoconferencing services through a number of monthly and annual subscription plans. Zoom offers a free basic videoconferencing plan that includes unlimited one-on-one and group videoconferencing for up to 40 minutes and 100 participants. It also offers three tiers of paid plans based on the number of features and host licenses provided, with minimum monthly subscription fees of \$14.99 (Pro), \$199.90 (Business), and \$999.50 (Enterprise).

8. Zoom routinely collects certain information about users, including: first and last name; email address; user name and password; approximate location; date of birth; technical information about users' devices, network, and internet connection; and in the case of a paid subscription, billing address and payment card information of the account holder. Zoom also collects and stores event details for all Zoom Meetings, including the date, time, and length of Meetings; the Meeting participants' user names; and each participant's answers to any polling questions asked during a Meeting. Finally, Zoom also collects and stores information shared while using the service, such as recorded Meetings that users store on Zoom's cloud storage, voice mails, chat and instant messages, files, and whiteboards.

9. As of July 2019, Zoom had approximately 600,000 paid customers of its videoconferencing services. Approximately 88% of those customers were small businesses with ten or fewer employees.

Complaint

10. In December 2019, approximately 10 million people worldwide participated in a Zoom Meeting each day. By April 2020, that number had skyrocketed to 300 million daily meeting participants worldwide, in large part due to an increased demand for videoconferencing services as a result of social distancing recommendations and local government stay-at-home orders related to the novel coronavirus pandemic. In addition to Zoom's traditional business customers, individuals, doctors, mental health professionals, schools, and others began to use Zoom's videoconferencing services in greater numbers.

11. Users share sensitive information during Zoom meetings. This can include financial information, health information, proprietary business information, and trade secrets. For example, Zoom has been used for therapy sessions, Alcoholics Anonymous meetings, and telehealth appointments.

12. As reflected in Zoom's Security Guide, the security of users' Zoom communications relies not only on its Meeting encryption or similar features, but also on its internal network security. Malicious actors who infiltrate Zoom's internal network could gain access to Zoom's administrative controls and compromise Zoom users' personal information. Despite this, Zoom, among other things, has:

- a. Failed to implement a training program on secure software development principles;
- b. Failed to test, audit, assess, or review its applications for security vulnerabilities at certain key points, such as prior to releasing software updates, including failing to ensure that its software is free from commonly known or reasonably foreseeable attacks, such as "Structured Query Language" (SQL) injection attacks and "Cross-Site Scripting" (XSS) attacks;
- c. Failed to monitor service providers or other contractors who have access to Zoom's network;
- d. Failed to secure remote access to its networks and systems through multi-factor authentication or similar technology;
- e. Failed to use readily available measures to safeguard against anomalous activity and/or cybersecurity events across all of Zoom's systems, networks, and assets within those networks, including monitoring all of Zoom's networks and systems at discrete intervals, properly configuring firewalls, and segmenting its networks;
- f. Failed to implement a systematic process for incident response;
- g. Failed to implement a systematic process for inventorying, classifying, and deleting user data stored on Zoom's network; and

Complaint

- h. Been a year or more behind in patching software in its commercial environment.

Respondent's Deceptive and Unfair Privacy and Security Practices

13. Zoom has made numerous, prominent representations touting the strength of the privacy and security measures it employs to protect users' personal information. For example, Zoom has claimed on its website, in Security Guides, and in its privacy policy, that it takes "security seriously," that it "places privacy and security as the highest priority," and that it "is committed to protecting your privacy."

14. The privacy and security of video communications, including the level of encryption used to secure those communications, is important to users and their decisions about which videoconferencing platform to use, the price to pay for such services, and/or how they use those services. In numerous blog posts, Zoom has pointed to its security as a reason for potential customers to use Zoom's videoconferencing services. In a January 2017 blog post, "Zoom: The Fastest Growing App on Okta," Zoom specifically cited, based on customer feedback, its security feature of "end-to-end AES 256 bit encryption" as important to businesses and one of the reasons for Zoom's growth.

Zoom's Deceptive End-to-End Encryption Claims

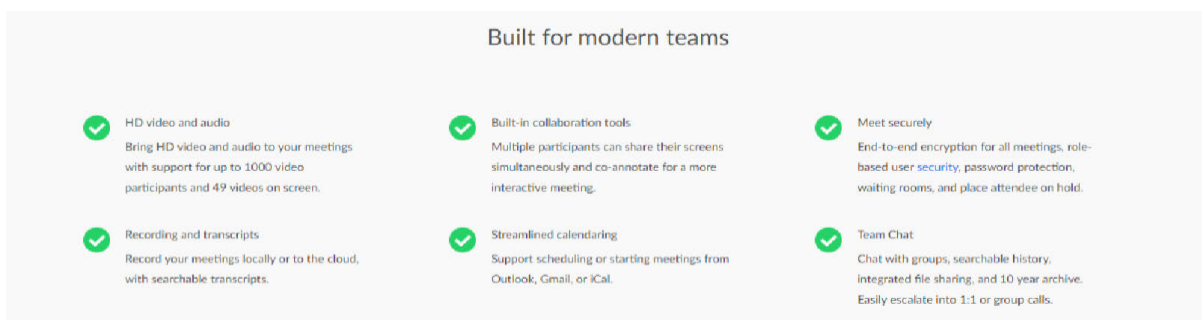
15. End-to-end encryption is a method of securing communications where an encrypted communication can only be deciphered by the communicating parties. No other persons can decrypt the communications because they do not possess the necessary cryptographic keys to do so. End-to-end encryption is intended to prevent communications from being read or modified by anyone other than the true sender and recipient(s).

16. Since at least June 2016, Zoom has represented in its App, on its website, in its Security Guides, in its HIPAA Compliance Guide, in blog posts, and in direct communications with customers, that it offered end-to-end encryption to secure videoconference communications between hosts and attendees during Zoom Meetings.

17. For example, Zoom has represented that it provided end-to-end encryption in the Zoom App. When a user hovered over a green padlock in the top left corner of a Meeting, the user would see a popup stating, "Zoom is using an end to end encrypted connection."

18. Zoom also has represented that it employed end-to-end encryption for Zoom Meetings on the "meetings" and "security" pages of its public website, available at zoom.us/meetings and zoom.us/security. For example, on its "meetings" webpage, Zoom claimed that it offered end-to-end encryption for "all meetings":

Complaint



19. Zoom has made similar representations in its Security Guides, which are available through its public website at www.zoom.us/security. In its June 2019 Security Guide, Zoom explained that Meeting hosts could “Enable an end-to-end (E2E) encrypted meeting.” Zoom likewise claimed in its June 2016 Security Guide that Meeting hosts could “Secure a meeting with end-to-end encryption (E2E).” Zoom also claimed that it used “industry-standard end-to-end” encryption with AES 256-bit encryption as a way for its healthcare customers to comply with the Health Insurance Portability and Accountability Act (HIPAA)’s Security Rule. The HIPAA Security Rule applies to certain healthcare entities and contains federally mandated standards for protecting individuals’ electronic personal health information.

20. For example, on the “healthcare” webpage of Zoom’s website, available at zoom.us/healthcare, Zoom claimed that its customers could “Achieve HIPAA (signed BAA) and PIPEDA/PHIPA compliance with complete end-to-end 256-bit AES encryption.” Zoom similarly explained in its June 2016 and July 2017 HIPAA Compliance Guides, available through its public website at zoom.us/healthcare, that its end-to-end encryption, among other security features, supported its healthcare customers’ compliance with the HIPAA Security Rule:

Security and Encryption

Only members invited by account administrators can host Zoom meetings in accounts with multiple members. The host controls meeting attendance through the use of meeting IDs and passwords. Each meeting can only have one host. The host can screen share or lock screen sharing. The host has complete control of the meeting and meeting attendees, with features such as lock meeting, expel attendees, mute/unmute all, lock screen sharing, and end meeting.

Zoom employs industry-standard end-to-end Advanced Encryption Standard (AES) encryption using 256-bit keys to protect meetings. Zoom encryption fully complies with HIPAA Security Standards to ensure the security and privacy of patient data.

21. In a January 2019 white paper entitled “End to End Encryption,” Zoom represented that it offered end-to-end encryption for Zoom Meetings as an “added layer of application security for Zoom meetings, webinars, and chat (instant messaging) sessions.” Zoom explained that end-to-end encryption meant that Zoom Meetings, webinars, and chat sessions could only be decrypted by “authenticated participant(s) who have the key required for decryption.” The white paper also explained that video, audio, and screen sharing were all “protected with the Advanced Encryption Standard (AES) 256-bit algorithm.”

Complaint

22. Zoom specifically touted its level of encryption as a reason for customers and potential customers to use Zoom’s videoconferencing services in numerous blog posts on its website. For example, in an April 24, 2017 blog post, “Zoom Reporting Live from American Telemedicine Association 2017,” Zoom promoted its “End-to-end AES 256-bit encryption of all meeting data and instant messages” as a reason for healthcare providers to use Zoom as their telehealth videoconferencing solution.

23. Additionally, in response to inquiries from customers or potential customers who contacted Zoom directly to ask about Zoom’s security practices and the level of encryption it employed for Zoom Meetings, Zoom informed them that it offers AES 256-bit, end-to-end encryption and directed them to its Security Guide that, as described above, made similar representations.

24. In fact, Zoom did not provide end-to-end encryption for any Zoom Meeting that was conducted outside of Zoom’s “Connector” product (which are hosted on a customer’s own servers), because Zoom’s servers—including some located in China—maintain the cryptographic keys that would allow Zoom to access the content of its customers’ Zoom Meetings. Zoom has acknowledged that its Meetings were generally incapable of end-to-end encryption in an April 2020 blog post by its Chief Product Officer:

In light of recent interest in our encryption practices, we want to start by apologizing for the confusion we have caused by incorrectly suggesting that Zoom meetings were capable of using end-to-end encryption. Zoom has always strived to use encryption to protect content in as many scenarios as possible, and in that spirit, we used the term end-to-end encryption. While we never intended to deceive any of our customers, we recognize that there is a discrepancy between the commonly accepted definition of end-to-end encryption and how we were using it. This blog is intended to rectify that discrepancy and clarify exactly how we encrypt the content that moves across our network.

<https://blog.zoom.us/wordpress/wpcontent/uploads/2020/04/zoom-servers-news.jpg>.

Zoom’s Deceptive Claims Regarding Level of Encryption

25. Encrypting communications with the Advanced Encryption Standard (AES) and a 256-bit encryption key can be an effective way to secure communications and prevent eavesdropping. The 256-bit encryption key refers to the length of the key needed to decrypt the communications. 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.

26. Since at least June 2015, Zoom has made numerous and prominent claims that it encrypted Zoom Meetings, in part, by using AES, with a 256-bit encryption key (“AES 256-bit Encryption” or “256-bit Encryption”).

27. For example, in a June 2015 blog post entitled “Why Zoom’s Security Features Matter for your Business,” available at <https://blog.zoom.us/wordpress/2015/06/17/why-zooms->

Complaint

security-matter-for-business/, Zoom explained that encryption was important for video communications because people “discuss sensitive things in unplanned moments,” and touted **“Zoom’s use of AES 256 encryption”** as making it **“it impossible for a hacker to grab anything outside of a hopelessly garbled transmission...”** (emphasis in original).

28. On the “security” page of Zoom’s website, available at zoom.us/security, Zoom also has claimed that it used 256-bit Encryption to protect user data:



29. Zoom likewise claimed that it uses 256-bit Encryption in its Security Guide and in its online Help Center. For example, Zoom’s June 2019 Security Guide stated, “Webinar contents and screen sharing are secured using AES 256 and communicate over secured network using 256-bit encryption standard.” In Zoom’s online Help Center, available at <https://support.zoom.us/hc/en-us/articles/201362723-Encryption-for-Meetings>, Zoom answered a “Frequently Asked Question[]” about its Meeting encryption by explaining, in part, that its Meetings were encrypted “by default” with AES 256-bit Encryption:

Encryption for Meetings

Overview

By default, Zoom encrypts in-meeting and in-webinar presentation content at the application layer using TLS 1.2 with Advanced Encryption Standard (AES) 256-bit algorithm for the Desktop Client.

30. In fact, Zoom used a lower level of encryption for securing Zoom Meetings, AES 128-bit encryption in Electronic Code Book (“ECB”) mode. AES 128-bit encryption uses a shorter encryption key than AES 256-bit Encryption, and therefore provides less confidentiality protection because there are fewer possible values for the 128-bit key than for a 256-bit key. Reflecting the comparative strength of AES 256-bit Encryption and AES 128-bit Encryption, the National Security Agency has reported that AES 256-bit Encryption may be used for securing “TOP SECRET” materials, whereas AES 128-bit encryption may only be used for securing “SECRET” communications.

Complaint

Zoom's Deceptive Claims Regarding
Secure Storage for Zoom Meeting Recordings

31. Zoom offers customers the ability to record their Zoom Meetings and store such recordings on either the host's local device or, for paying customers, in Zoom's secure cloud storage ("Cloud Recordings").

32. In Zoom's June 2019 Security Guide, Zoom claims that Cloud Recordings are processed and stored in Zoom's cloud "after the meeting has ended," where they "are stored encrypted as well." Zoom's June 2016 Security Guide similarly claimed that Cloud Recordings "are processed and securely stored in Zoom's cloud once the meeting has ended."

33. In fact, recorded Meetings are kept on Zoom's servers for up to 60 days, unencrypted, before Zoom transfers the recordings to its secure cloud storage, where they are then stored encrypted.

Zoom's Unfair Circumvention of a
Third-Party Privacy and Security Safeguard

34. In July 2018, Zoom updated its App for Mac computers by deploying a web server onto users' computers—without adequate user notice or consent—in order to circumvent a security and privacy safeguard in Apple's Safari browser. Specifically, 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.

35. 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 App from launching.

36. To avoid this dialogue box, Zoom issued a manual update in July 2018 for its Zoom App for Mac desktop computers that secretly deployed a web server, called the "ZoomOpener," as a means to bypass the new privacy and security safeguard.

37. The ZoomOpener web server was installed on users' Mac computers and operated in the computer's background. When it detected a request to join a Zoom Meeting, the web server bypassed the new Safari browser safeguard to directly launch the Zoom App. It would then automatically join the user to the Zoom Meeting and, if the user had not changed her default video settings, automatically activate the user's webcam. Zoom automatically activated users' webcams immediately upon their joining a Meeting unless users changed their default video settings by logging into their Zoom account, going to their "preferences," clicking on "video," and then finding and clicking on the box, "Turn off my video when joining a meeting."

38. The ZoomOpener web server harmed consumers by limiting the intended benefit of a privacy and security safeguard provided by their Safari browser. Zoom did not implement

Complaint

any compensating measures to replace the privacy and security protections that it had circumvented, nor did Zoom take any steps to address the risks that malicious actors could exploit the ZoomOpener web server and harm users. Without the circumvented Safari safeguard, one wrong click could expose consumers to remote video surveillance by strangers through their computers' webcams.

39. For example, malicious actors could exploit this vulnerability by using a phishing attack, a common form of cyberattack that typically entails a criminal sending out thousands of emails that pretend to be from a legitimate source in order to direct recipients to a bogus website where the criminal can capture personal information or engage in other malicious activity. Here, the phishing email could trick consumers into clicking on an innocuous-looking link that does not appear to be a Zoom Meeting invite. This link could then direct the consumer to an otherwise benign-looking website that has a Zoom Meeting embedded in it. Zoom Meetings can be embedded in websites through the use of the iframe HTML tool, which allows a segment of a website to display content from another source without leaving the original website (such as a YouTube video playing on a host's website).

40. Without the consumer taking any additional steps, the ZoomOpener web server would automatically join the consumer to the Zoom Meeting and activate her webcam—without the user's consent and perhaps without even realizing it. Merely leaving the website would not exit the Meeting or disable the webcam. Had Zoom not circumvented the Safari safeguard, users would have been alerted to the Zoom Meeting and would have had to give their permission before being joined to the Meeting.

41. In addition to bypassing the Safari browser safeguard, the ZoomOpener web server also harmed users by introducing two additional security vulnerabilities. First, the web server exposed some users to a potential Remote Control Execution (RCE) attack because the ZoomOpener web server would download and install software updates, including potentially malicious code, without properly validating that it was downloading the software from a trusted source. This code could then allow the malicious actor to execute code on the user's computer. On July 9, 2019, Zoom posted information about this vulnerability on its website, available at <https://support.zoom.us/hc/en-us/articles/360031245072-Security-CVE-2019-13567>, where it characterized the vulnerability as having "High Severity." Second, the ZoomOpener web server exposed users to a local denial of service ("DoS") attack where a hacker could potentially target a Zoom user with an endless loop of invalid Meeting join requests that would effectively cause the targeted machine to lock up.

42. As discussed in further detail in Paragraphs 49-52 below, Zoom did not notify users that its manual software update would install the ZoomOpener web server on their Mac computers. Nor did Zoom provide users with any information about the web server's operation, including the fact that it would bypass a Safari privacy and security safeguard.

43. In addition to bypassing the Safari privacy and security safeguard to launch Zoom Meetings, the ZoomOpener web server had a second function: to reinstall the Zoom App. Specifically, if a Mac user deleted the Zoom App in accord with Apple's instructions for deleting

Complaint

apps, the ZoomOpener web server would nevertheless remain on users' computers. If the user later clicked on a Zoom Meeting invite or visited a website with an embedded Zoom Meeting, the web server would secretly reinstall the Zoom App—without any user interaction—and automatically join the user to the Meeting.

44. Because the ZoomOpener web server remained and continued to function on users' computers even after the Zoom App was deleted, the vulnerabilities described in Paragraphs 39-41 persisted after users deleted the Zoom App.

45. Zoom's deployment of the ZoomOpener web server—without adequate notice or consent—to circumvent a browser privacy and security safeguard, while also exposing users to additional security vulnerabilities as described in Paragraph 41, reflects Zoom's poor privacy and security practices. As described more fully in Paragraph 12, Zoom's security policies and practices have been inconsistently applied across its systems, and it has lacked an effective training program on secure software development principles.

46. The ZoomOpener web server's vulnerabilities impacted over 3.8 million U.S. consumers who had the ZoomOpener web server secretly installed on their Mac computers.

47. After a security researcher published information about the web server in early July 2019, Zoom issued a patch to remove the ZoomOpener web server from users' computers. A day later, Apple, Inc. issued a silent operating system update to protect Mac users from the ZoomOpener web server and automatically removed the web server from their computers. Although Zoom still allows customers to embed Meetings on their own websites, Zoom introduced a new video preview screen so that users would be able to see their own webcam stream before joining a Meeting.

48. Consumers could not reasonably have avoided the harms resulting from the secret deployment of the ZoomOpener web server. Zoom did not inform users that it was installing the ZoomOpener web server on their computer or otherwise provide any information about its operation, and it did not inform users that the web server would remain on their computers after they uninstalled the Zoom App. Consumers also had no way of independently knowing about the web server's security vulnerabilities. This substantial injury is not offset by countervailing benefits to consumers or competition.

Zoom's Deceptive Deployment of the ZoomOpener Web Server

49. The ZoomOpener web server was deployed as part of a manual software update for Zoom's Mac App on July 1, 2018 ("Web Server Update"). Within the Zoom App, Zoom notifies users of software updates in several ways: a pop up window; a blue bar that informs users that new updates are available; and through a "check for updates" feature available through a drop down menu under the user's profile icon.

50. The pop-up notification and "check for updates" feature both provide users with "Release Notes" that give information about the update, such as a listing of new and enhanced

Complaint

features included in the update as well as any resolved issues, such as bug fixes. They also include an “Update” button for users to click and manually update their software.

51. As reflected in the Release Notes shown below, Zoom told users that the Web Server Update would fix minor bugs. Zoom failed to disclose, or disclose adequately, that the update would install a local hosted web server, that the web server would circumvent a Safari browser privacy and security safeguard, or that it would remain on users’ computers even after they had deleted the App:

July 1, 2018 Version **4.1.27695.0702**

Download Type: Manual

Resolved issues

- **Minor bug fixes**

52. The omitted information was not available to users from any other source, and would have been material to their decision on whether or not to install the update. Indeed, when Zoom announced in early July 2019 that it would update its software to remove the ZoomOpener web server, it reported that it was doing so in response to customer feedback.

53. For example, some consumers made the following public comments about Zoom’s secret deployment of the ZoomOpener web server:

- “I think they [Zoom] need to be made aware that this isn't acceptable...I do not believe this is a fair trade-off - allowing any arbitrary web site local control of privileged software installed on my machine - because Safari offers a security prompt (specifically so that any arbitrary web site does not gain control of privileged software on my machine). I will be switching ~/.zoomus/ZoomOpener.app off, and considering other options until it has been fixed.”
- “I liked Zoom when I used it a couple of times, but the reinstall ‘feature’ [of the ZoomOpener web server] is a huge violation of my trust. Software from the company behind it will not touch my system anymore.”
- “I cancelled my subscription because of [Zoom’s installation of the ZoomOpener web server]... This should not be considered OK.”

Complaint

VIOLATIONS OF THE FTC ACT**Count I****Deceptive Representation Regarding End-to-End Encryption**

54. As alleged in Paragraphs 14-23, Zoom has represented, directly or indirectly, expressly or by implication, that it employed end-to-end encryption to secure the content of communications between participants using Zoom's video conferencing service.

55. In fact, as described in Paragraph 24, Zoom did not employ end-to-end encryption to secure the content of communications between participants using Zoom's video conferencing service. Therefore, the representation set forth in Paragraph 54 is false or misleading.

Count II**Deceptive Representation Regarding Level of Encryption**

56. As alleged in Paragraphs 25-29, Zoom has represented, directly or indirectly, expressly or by implication, that it employed 256-bit Encryption to secure the content of communications between participants using Zoom's video conferencing service.

57. In fact, as described in Paragraph 30, Zoom did not employ 256-bit Encryption to secure the content of communications between participants using Zoom's video conferencing service. Therefore, the representation set forth in Paragraph 56 is false or misleading.

Count III**Deceptive Representation Regarding
Secured Cloud Storage for Recorded Meetings**

58. As alleged in Paragraphs 31-32, Zoom has represented, directly or indirectly, expressly or by implication, that recorded Meetings are stored encrypted in Zoom's cloud storage immediately after a Meeting has ended.

59. In fact, as set forth in Paragraph 33, recorded Meetings are not stored encrypted in Zoom's cloud storage immediately after a Meeting has ended. Therefore, the representation set forth in Paragraph 58 is false or misleading.

Count IV**Unfair Circumvention of Third-Party Privacy and Security Safeguard**

60. As alleged in Paragraphs 34-48, Zoom installed the ZoomOpener web server, without adequate notice or consent, to circumvent a browser privacy and security safeguard and did not implement measures to replace the circumvented privacy and security protections.

61. Respondent's actions caused or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid and that is not outweighed by countervailing benefits to

Decision and Order

consumers or competition. Therefore, the practice set forth in Paragraph 60 is an unfair act or practice.

Count V
Deceptive Failure to Disclose

62. As alleged in Paragraph 51, in connection with the advertising, marketing, promotion, offering for sale, or sale of its video conferencing products, Respondent represented, directly or indirectly, expressly or by implication, that Zoom was updating its Mac App in order to resolve minor bug fixes.

63. In numerous instances in which Respondent made the representation set forth in Paragraph 62, Respondent failed to disclose or disclose adequately that the update would deploy a local hosted 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 the Zoom App.

64. In light of the representation described in Paragraph 62, Respondent's failure to disclose or disclose adequately the material information as set forth in Paragraph 63 constitutes a deceptive act or practice in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

Violations of the FTC Act

65. The acts and practices of Zoom as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

THEREFORE, the Federal Trade Commission this nineteenth day of January 2021, has issued this Complaint against Respondent.

By the Commission, Commissioners Chopra and Slaughter dissenting.

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.

Decision and Order

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

Decision and Order

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.

Decision and Order

- 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:

Decision and Order

- 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

Decision and Order

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

Decision and Order

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

Decision and Order

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

Decision and Order

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

Decision and Order

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, Docket No. C-4731.” 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.

Decision and Order

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, Docket No. C-4731."

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

Decision and Order

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, Docket No. C-4731."

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

Decision and Order

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, Docket No. C-4731.”

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;

Decision and Order

- 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

Statement of the Commission

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 January 19, 2041, 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, Commissioners Chopra and Slaughter dissenting.

**MAJORITY STATEMENT OF CHAIRMAN JOSEPH J. SIMONS, COMMISSIONER
NOAH JOSHUA PHILLIPS, AND COMMISSIONER CHRISTINE S. WILSON**

At a time when millions of Americans are using videoconferencing services on a daily basis, the settlement that the Commission announces today ensures that Zoom will prioritize consumers' privacy and security. The Commission's complaint alleges that Zoom made misrepresentations regarding the strength of its security features and implemented a software update that circumvented a browser security feature. The proposed order provides immediate and important relief to consumers, addressing this conduct. The order requires that Zoom establish and implement a comprehensive security program that includes detailed and specific security measures. These obligations include reviews of all new software for common security

Dissenting Statement

vulnerabilities; quarterly scans of its internal network and prompt remediation of critical or severe vulnerabilities; and prohibitions against privacy and security misrepresentations.¹ This order will enable the Commission to seek significant penalties for noncompliance. This settlement provides critical, and timely, relief.

We are confident that the proposed relief appropriately addresses the conduct alleged in the complaint and is an effective, efficient resolution of this investigation. Our dissenting colleagues suggest additional areas for relief that likely would require protracted litigation to obtain. Given the effective relief this settlement provides, we see no need for that. Hundreds of millions of people use Zoom on a daily basis, often for free or through month-to-month contracts. We feel it is important to put in place measures to protect those users' privacy and security now, rather than expend scarce staff resources on speculative, potential relief that a Court would not likely grant, given the facts here.² Our goal is a safe and secure Zoom that can continue to provide essential services to enable Americans to conduct business, engage in learning, participate in religious services, and stay connected. We applaud the FTC Staff for their professional and expeditious work to achieve this settlement in the midst of the pandemic. This case reflects the Commission's ongoing commitment to work on behalf of consumers to respond to the panoply of new challenges presented by COVID-19.

DISSENTING STATEMENT OF COMMISSIONER ROHIT CHOPRA**Summary**

- When companies deploy deception, this harms customers and honest competitors, and it distorts the marketplace. This is particularly problematic when it comes to the digital economy.
- Zoom's alleged security failures warrant serious action. But the FTC's proposed settlement includes no help for affected parties, no money, and no other meaningful accountability.

1 Although the complaint does not allege privacy violations, the order includes targeted fencing in relief providing privacy protections to consumers. For example, it prohibits Zoom from misrepresenting its privacy practices, and requires Zoom to implement changes to its naming procedures for saving or storing recorded videoconference meetings, and to develop data deletion policies and procedures. These and other requirements serve to protect consumers' privacy as well as the security of their information and communications.

2 Our dissenting colleagues also argue that the settlement is insufficient because it does not require Zoom to notify consumers of its past misconduct. The conduct at issue was broadly publicized and we believe the Commission's press release and business and consumer education provide ample information for consumers to learn more.

Dissenting Statement

- The FTC’s status quo approach to privacy, security, and other data protection law violations is ineffective. However, Commissioners can take a series of concrete steps to change this.

Introduction

Sometimes a new product becomes inextricably linked to the brand that made it popular. Kleenex, Band-Aids, and Frisbees are examples where the company became synonymous with the product.¹ This is particularly true in the digital economy where products can improve the use and capability of technology to the point of transforming its role in everyday life. We use “Google” as a verb when referring to use of a search engine. We “Uber” when we need a ride across town. And now, we “Zoom” when referring to videoconferencing. If becoming a verb threatens a trademark, firms fight against it. If it means becoming the default product in a market, they fight for it. But, profiting through unlawful means must come with real consequences.

Zoom (NASDAQ: ZM) did not invent web-based video conferencing. Indeed, there are many other players in the market. But Zoom succeeded in becoming the “default” for many businesses, both large and small, capturing a significant market share despite a crowded field. However, the allegations in the FTC’s complaint raise questions whether Zoom’s success – and the tens of billions of dollars of wealth created for its shareholders and executives in a short period of time – was advanced through fair play.² In my view, the evidence suggests that deception helped to create this windfall.

With businesses, families, schools, and even governments using Zoom to share extremely sensitive information, the alleged security vulnerabilities of this video conferencing platform raise major concerns, including threats to our privacy³ and national security.⁴

Today, the Federal Trade Commission has voted to propose a settlement with Zoom that follows an unfortunate FTC formula. The settlement provides no help for affected users. It does nothing for small businesses that relied on Zoom’s data protection claims. And it does not require Zoom to pay a dime. The Commission must change course.

1 Mark Abadi, *Taser, Xerox, Popsicle, and 31 more brands-turned-household names*, BUSINESS INSIDER (June 3, 2018), <https://www.businessinsider.com/google-taser-xerox-brand-names-generic-words-2018-5>.

2 Richard Waters, *Zoom to cash in on pandemic success with apps and events*, FINANCIAL TIMES (Oct. 14, 2020), <https://www.ft.com/content/f1731672-e965-48a1-9362-bab122fc9bf4>.

3 In her voting statement, Commissioner Rebecca Kelly Slaughter details some of the key intersections between privacy and security.

4 Sonam Sheth, *Foreign intelligence operatives are reportedly using online platforms and video-conferencing apps like Zoom to spy on Americans*, BUSINESS INSIDER (Apr. 9, 2020), <https://www.businessinsider.com/foreign-intelligence-agents-china-spying-on-americans-zoom-2020-4>.

Dissenting Statement

Deception Distorts Competition

When companies need to act quickly to exploit an opportunity, deploying deception to steal users or sales from competing players is tantalizing. When video conferencing became a necessity for many businesses and families, existing players saw a potential gold mine. Even though we can all technically use multiple videoconferencing platforms as participants, a videoconferencing provider's monetization will largely be driven by how many businesses adopt its offering as their enterprise videoconferencing solution.⁵ FTC prohibitions on unfair or deceptive practices are supposed to temper the temptation to deceive customers.

Before the pandemic, Zoom primarily focused on business customers. Small and large businesses alike were looking for ways to connect with clients and business partners through video conferencing. Zoom competed with Microsoft's Skype, Microsoft's Teams, Cisco's WebEx, BlueJeans, and many other products. Comparison guides point out the different strong points of each service – from encryption to price.⁶ In the summer of 2019, Zoom had over 600,000 customers that paid fees to use Zoom's services.⁷ These customers were overwhelmingly small businesses.⁸

Small businesses often don't have employees dedicated to information security or even to information technology more broadly. That's why they rely on representations made by those they purchase software and services from. Many businesses want to ensure that any software application they use, including any video conferencing solution, comes with meaningful security standards. Zoom had to respond to this critical customer need if it was going to compete. Once the pandemic shut down workplaces across the country, businesses needed to find a reliable solution that was also secure. Many chose Zoom.⁹

Zoom sold its customers on the idea that it was an easy-to-use service that took "security seriously." However, when examining the company's engineering and product decisions, a different reality emerges. For example, as the complaint alleges, Zoom installed a web server onto users' computers, without permission, as an end-run that would circumvent a browser security feature – all to avoid an extra dialogue box.¹⁰ Zoom went further: even if you managed

5 Zoom Video Communications, Inc., Oct. 2019 Quarterly Report (Form 10-Q) (Dec. 9, 2019), <https://www.sec.gov/ix?doc=/Archives/edgar/data/1585521/000158552119000059/zm-20191031.htm>.

6 Kari Paul, *Worried about Zoom's privacy problems? A guide to your video-conferencing options*, THE GUARDIAN (Apr. 9, 2020), <https://www.theguardian.com/technology/2020/apr/08/zoom-privacy-video-chat-alternatives>.

7 Compl., *In the Matter of Zoom Video Communications, Inc.*, Comm'n File No. 1923167 (Nov. 9, 2020).

8 *Id.*

9 Matt Torman, *5 Reasons Why Zoom Will Benefit Your Small Business*, ZOOM (Jan. 24, 2020), <https://blog.zoom.us/zoom-video-communications-small-business-benefits/>.

10 Compl., *supra* note 7.

Dissenting Statement

to uninstall Zoom, it would not remove the web server.¹¹ And that web server could secretly re-install Zoom, even without your permission.¹² This is not just troubling conduct – this is what some have called “malware-like” behavior.¹³

This fervent attention to detail – going to great lengths to avoid a single dialogue box – did not extend to the security features it touted in sales materials.¹⁴ The FTC’s complaint details a litany of serious security allegations, from not using what is “the commonly accepted definition” of end-to-end encryption to being a year or more behind in patching software in its commercial environment.¹⁵

Zoom’s Windfall

Zoom has “cashed in” on the pandemic.¹⁶ While Zoom doesn’t publicly share its total number of users, the company has confirmed that it has nearly four times the number of customers with 10 or more employees than they had at this time a year ago.¹⁷ Their stock value has soared.¹⁸ Zoom’s CEO, Eric Yuan, has increased his net worth by almost \$16 billion *since March*, and is now one of the wealthiest individuals in America.¹⁹

Zoom can now use this new market penetration to increase monetization for users who currently do not pay any fees. With the pandemic-driven expansion, Zoom has announced that they’re going to make a platform pivot and begin to offer an app marketplace and a paid events

11 David Murphy, *Remove Zoom From Your Mac Right Now*, LIFEHACKER (July 9, 2020), <https://lifehacker.com/remove-zoom-from-your-mac-right-now-1836209383>.

12 *Id.*

13 Jacob Kastrenakes, *Zoom saw a huge increase in subscribers — and revenue — thanks to the pandemic*, THE VERGE (June 2, 2020), <https://www.theverge.com/2020/6/2/21277006/zoom-q1-2021-earnings-coronavirus-pandemic-work-from-home>.

14 Compl., *supra* note 7.

15 Michael Lee & Yael Grauer, *Zoom Meetings Aren’t End-to-End Encrypted, Despite Misleading Marketing*, THE INTERCEPT (Mar. 31, 2020), <https://theintercept.com/2020/03/31/zoom-meeting-encryption/>; Compl., *supra* note 7; Oded Gal, *The Facts Around Zoom and Encryption for Meetings/Webinars*, ZOOM (Apr. 1, 2020), <https://blog.zoom.us/facts-around-zoom-encryption-for-meetings-webinars/>.

16 Richard Waters, *Zoom to cash in on pandemic success with apps and events*, FINANCIAL TIMES (Oct. 14, 2020), <https://www.ft.com/content/f1731672-e965-48a1-9362-bab122fc9bf4>.

17 *Id.*

18 *Id.*

19 Taylor Nicole Rogers, *Meet Eric Yuan, the founder and CEO of Zoom, who has made over \$12 billion since March and now ranks among the 400 richest people in America*, BUSINESS INSIDER (Sep. 9, 2020), <https://www.businessinsider.com/meet-zoom-billionaire-eric-yuan-career-net-worth-life>; Kerry A. Dolan et al., *The Forbes 400: The Definitive Ranking of the Wealthiest Americans in 2020*, FORBES (Sep. 8, 2020), <https://www.forbes.com/profile/eric-yuan/?list=forbes-400&sh=474b78c761bf>.

Dissenting Statement

platform.²⁰ Zoom disclosed to its investors how a shift to a “platform and sales model allow[s] us to turn a single non-paying user into a full enterprise deployment.”²¹

Zoom stands ready to emerge as a tech titan. But we should all be questioning whether Zoom and other tech titans expanded their empires through deception.²² Zoom could have taken the time to ensure that its security was up to the right standards. But, in my view, Zoom saw the opportunity for massive growth by quickly leaping into the consumer market, allowing it to rapidly emerge as the new way to virtually celebrate birthdays and weddings and further solidify itself into our lives. But had Zoom followed the law, it might all be different.

Status Quo Approach to Privacy and Security Settlements

In matters like these, investigations should seek to uncover how customers were baited by any deception, how a company gained from any misconduct, and the motivations for this behavior. This approach can help shape an effective remedy. While deciding to resolve a matter through a settlement, regulators and enforcers must seek to help victims, take away gains, and fix underlying business incentives.

Of course, all settlements involve tradeoffs, but like other FTC data protection settlements, the FTC’s proposed settlement with Zoom accomplishes none of these objectives. This is particularly troubling given the nature of the alleged deception. Key features of the FTC’s proposed settlement include:

No help. Small businesses that purchased Zoom services or signed long-term contracts based on false representations are not even addressed in the Commission’s order. They will not have the ability to be released from any contracts, seek refunds, or get credit toward future service. Similarly, Zoom’s law-abiding competitors and other consumers affected by the alleged misconduct will not get anything to address how they were harmed.

No notice. The targets of deception deserve the dignity of knowing that the product they were using did not use the security features that were advertised. Notice also provides information on whether or not users need to take any specific further actions to protect themselves or their place of business. This is especially critical in cases where individuals may not know if they are affected. In this matter, Zoom’s technology was integrated into white label products that may not use Zoom’s brand. Notice is also helpful when victims receive no restitution.

²⁰ *Supra* note 16.

²¹ Zoom Video Communications, Inc., Quarterly Report (Form S-1) (Dec. 21, 2018), <https://www.sec.gov/Archives/edgar/data/1585521/000095012318012479/zoom1.htm>.

²² Decision and Order, *In the Matter of Google Inc.*, Comm’n File No. 1023136 (Oct. 24, 2011), <https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110330googlebuzzagreeorder.pdf>; Decision and Order, *In the Matter of Facebook, Inc.*, Comm’n File No. 0923184 (July 27, 2012), <https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf>.

Dissenting Statement

No money. In my view, the evidence is clear that Zoom obtained substantial benefits through its alleged conduct. However, the resolution includes no monetary relief at all, despite existing FTC authority to seek it in settlements when conduct is dishonest or fraudulent. If the FTC was concerned about its ability to seek adequate monetary relief, it could have partnered with state law enforcers, many of whom can seek civil penalties for this same conduct.

No fault. The Commission's order includes no findings of fact or liability. In other words, Zoom admits nothing and the Commission's investigation makes no significant conclusions. This will make it more difficult for affected parties to exercise any contractual rights or seek help through private actions.

Earlier this year, after a number of security concerns emerged, the Attorney General of New York quickly took action, and Zoom signed a voluntary compliance agreement, which requires certain third-party reports and compliance with additional standards.²³ The FTC's proposed settlement terms add some requirements to what Zoom has already agreed to with New York, largely involving additional independent monitoring and paperwork submissions. It is not clear to me that these new obligations are actually changing the way Zoom does business. In fact, Zoom may already be retaining third parties to assist with compliance as part of its contractual obligations with its largest customers.

Recommendations to Restore Credibility

To protect the public and promote fair markets, the FTC must be a credible law enforcement agency, especially when it comes to large players in digital markets. Our recent law enforcement actions raise questions that warrant careful attention if we aspire to be an effective enforcer. Below are some of the tangible steps the Commission should pursue:

1. *Strengthen orders to emphasize more help for individual consumers and small businesses, rather than more paperwork.*

When consumers and small businesses are the targets of unlawful data protection practices, the FTC's status quo approach often involves requiring the company engaged in misconduct to follow the law in the future and submit periodic paperwork. In certain orders, the Commission requires the retention of a third-party assessor, which the company might already be doing.

The FTC should focus its efforts on ensuring resolutions lead to meaningful help and assistance to affected consumers and small businesses. For example, the Commission could seek requirements that defendants respond to formal complaints and inquiries. This assists consumers while also allowing the Commission to track emerging harms and how the company is remediating them.

23 Press Release, N.Y. Att'y Gen., Attorney General James Secures New Protections, Security Safeguards for All Zoom Users (May 7, 2020), <https://ag.ny.gov/press-release/2020/attorney-general-james-secures-new-protections-security-safeguards-all-zoom-users>.

Dissenting Statement

Another way to help affected consumers and businesses is to order releases from any long-term contractual arrangements. When customers are baited with deceptive claims, it would be appropriate to allow them to be released from any contract lock-in or otherwise amend contractual terms to make customers whole. This would also help honest competitors regain some of the market share improperly diverted by deceptive conduct.

The Commission should seek notices to affected parties, so that these individuals and businesses can determine whether they need to take any action and whether they want to continue to do business with a company that engaged in any wrongdoing.

2. *Investigate firms comprehensively across the FTC's mission.*

The FTC is a unique institution with legal authorities related to data protection, consumer protection, and competition, all under one roof, rather than divided up across multiple agencies. It is critical that the agency use its authority to deter unfair or deceptive conduct in conjunction with our authority to deter unfair methods of competition. The agency can do more to comprehensively use its authorities across its mission, particularly when unfair or deceptive practices can advance dominance in digital markets. When we do not, investigations may result in ineffective resolutions that fail to fix the underlying problems and may increase the likelihood of recidivism. The Commission may need to reorganize its offices and divisions to ensure investigations are comprehensive.

3. *Diversify the FTC's investigative teams to increase technical rigor.*

Engineers, designers, and other technical experts can offer major contributions to our investigative teams. Many of the cases previously pursued by the FTC were the result of press coverage from technical experts, especially security researchers. In fact, an independent researcher working in his private capacity was one of the first to discover a serious vulnerability in Zoom's product.²⁴

Many of our peer agencies around the world approach investigations with diverse, interdisciplinary teams. Unfortunately, the Commission has deprived our litigators and enforcement attorneys of this needed expertise. The Commission should restore the role of the Chief Technologist and make a concerted effort to increase the proportion of technologists and others with technical knowledge in our investigative teams. If these individuals play meaningful leadership roles in our investigations, the agency can be much more effective.

With these technical skills and leadership in place, the Commission could proactively review the dominant digital products and services rather than primarily following up on concerning media reports after sensitive information or access has been at risk.

²⁴ The independent research solicited readers for contributions to assist with his work and pay off his student loans. Jonathan Leitschuh, *Zoom Zero Day: 4+ Million Webcams & maybe an RCE? Just get them to visit your website!*, INFOSEC WRITE-UPS (July 8, 2019), <https://medium.com/bugbountywriteup/zoom-zero-day-4-million-webcams-maybe-an-rce-just-get-them-to-visit-your-website-ac75c83f4ef5>.

Dissenting Statement

4. *Restate existing legal precedent into clear rules of the road and trigger monetary remedies for violations.*

Markets benefit when there are simple, clear rules of the road. This allows honest businesses to know what is and is not permissible. This especially helps small businesses and startups. On the other hand, ambiguity helps large incumbents who can hire lawyers and lobbyists to sidestep their obligations. The FTC can promote fair markets by restating accepted legal precedent and past Commission experience through an agency rulemaking. These would create no new substantive obligations on market participants. But once restated and enforced, violations trigger significant monetary relief.

Under the FTC Act, the Commission has a number of authorities to seek monetary relief. While one of these authorities, Section 13(b), is under considerable scrutiny in the courts, the Commission can also seek money by restating existing legal precedent through a rulemaking. When the Commission has issued prior orders for past misconduct in the market or there is other information indicating a widespread pattern of unfair or deceptive conduct, Section 18 of the FTC Act authorizes the Commission to define what constitutes an unfair or deceptive practice by rule. Violations of these rules can trigger liability for redress, damages, penalties, and more.

Over the years, the Commission has finalized a substantial number of orders related to data protection, including privacy and data security. There have also been developments in case law in the courts. The Commission should consider restating this past precedent into a rule under Section 18 or other appropriate statutes to provide clear guidance and systematically deter unlawful data protection practices.²⁵

5. *Demonstrate greater willingness to pursue administrative and federal court litigation.*

Congress intended for the FTC to serve as an expert agency that analyzes emerging business practices and determines whether they might be unfair or deceptive. Administrative litigation and final Commission orders can provide important guidance to the marketplace on the agency's analytical approach. It can also serve as the basis for triggering financial liability for other market actors, pursuant to the Commission's Penalty Offense Authority.²⁶

Federal court litigation pursued by our staff has contributed to strong outcomes and important development of the law. For example, in 2012, the FTC took action against Wyndham Hotels, a major hospitality chain the Commission charged with employing unfair data practices.

25 Statement of Commissioner Rohit Chopra Regarding the Report to Congress on Protecting Older Consumers, Comm'n File No. P144400 (Oct. 19, 2020), https://www.ftc.gov/system/files/documents/public_statements/1581862/p144400choprastatementolderamericansrpt.pdf.

26 See Rohit Chopra & Samuel A.A. Levine, *The Case for Resurrecting the FTC Act's Penalty Offense Authority* (Oct. 29, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3721256.

Dissenting Statement

Wyndham Hotels waged an aggressive defense, challenging the FTC's theories before the District Court and the Third Circuit Court of Appeals. The court's ruling cemented the Commission's ability to target lax data security practices under existing law.

The public benefits from the work of the FTC's talented investigators and litigators across the agency, and as Commissioners, we should have confidence that they can hold accountable even the largest players in the economy. But recently, when it comes to data protection, FTC Commissioners have rarely voted to authorize agency staff to sue national players for misconduct. We must do more to safeguard against any perception about the agency's unwillingness to litigate.

6. *Increase cooperation with international, federal, and state partners.*

When it comes to data protection abuses and other harmful practices by large technology firms, these concerns are increasingly global. The FTC can use its resources more effectively and obtain superior outcomes when it cooperates with other law enforcement partners.

In the Ashley Madison matter, the FTC partnered with the Office of the Privacy Commissioner of Canada, Office of the Australian Information Commissioner, and many state attorneys general. This action was the result of significant cooperation and ultimately led to a joint resolution.²⁷ Unfortunately, this is too rare.

The FTC can rely on key provisions of the U.S. SAFE WEB Act that allow the FTC to share information with foreign counterparts to combat deceptive or unfair practices that cross national borders. Domestically, agencies can form multistate working groups to combine resources and leverage a diverse set of legal authorities.

In the matter before the Commission today, the conduct at issue might have also violated state laws. Additional liability triggered by these laws could have led to a resolution with a far superior outcome. Instead, other law enforcement agencies both at home and abroad will likely need to continue to scrutinize Zoom's practices, given the FTC's proposed resolution.

In addition, the Commission needs to rethink its approach to enforcing privacy promises by large technology firms related to their participation in international agreements, such as the EU-U.S. Privacy Shield Framework. Zoom's conduct may have violated key aspects of the framework, and I believe the Commission should have taken action accordingly. The Commission should now fully cooperate with our international partners to ensure that they can proceed with appropriate sanctions.

27 Press Release, Fed. Trade Comm'n, Operators of AshleyMadison.com Settle FTC, State Charges Resulting From 2015 Data Breach that Exposed 36 Million Users' Profile Information (Dec. 14, 2016), <https://www.ftc.gov/news-events/press-releases/2016/12/operators-ashleymadisoncom-settle-ftc-state-charges-resulting>.

Dissenting Statement

7. *Determine whether third-party assessments are effective.*

A common provision in FTC orders requires the defendant to retain a third party to monitor compliance and the company's data protection protocols. However, it is unclear whether those assessments are truly effective when it comes to deterring or uncovering misconduct. For example, in the FTC's investigation of Facebook for compliance with its privacy obligations under a 2012 Commission order, the FTC alleged major violations of the order even though an independent third party, PriceWaterhouseCoopers (PwC), was supposedly watching over the company's compliance.²⁸

Additionally, the Commission's decision to not proactively make certain information about these third party reports public limits our ability to determine their effectiveness.²⁹ If independent researchers and journalists – often the ones who originally discovered data protection failures in the first place – had access to these reports, companies and third-party monitors might take them more seriously, which would help to fulfill the intended purpose of their efforts.

Conclusion

This year families have said their final goodbyes to loved ones over Zoom.³⁰ Desperate parents have propped their children in front of screens for school and hoped that they won't fall too far behind.³¹ Small businesses have been turned upside down by our new way of life and have fought for a chance at survival by switching to doing business virtually.³² But when tech companies cheat, rather than compete, and then face no meaningful accountability, all of us suffer.

I am concerned that Zoom simply thought that the FTC's law enforcement inquiry wasn't serious. That's probably why the company didn't even bother to disclose the agency's inquiry to

28 See Nitasha Tiku, *Facebook's 2017 Privacy Audit Didn't Catch Cambridge Analytica*, WIRED (Apr. 19, 2018), <https://www.wired.com/story/facebooks-2017-privacy-audit-didnt-catch-cambridge-analytica/>; See also Dissenting Statement of Commissioner Rohit Chopra In re Facebook, Inc., Comm'n File No. 1823109 (July 24, 2019), https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf.

29 Statement of Commissioner Rohit Chopra In the Matter of Uber Technologies, Inc., Comm'n File No. 1523054 (Oct. 26, 2018), https://www.ftc.gov/system/files/documents/public_statements/1418195/152_3054_c-4662_uber_technologies_chopra_statement.pdf.

30 Sarah Zhang, *The Pandemic Broke End-of-Life Care*, THE ATLANTIC (June 16, 2020), <https://www.theatlantic.com/health/archive/2020/06/palliative-care-covid-19-icu/613072/>.

31 Heather Kelly, *Kids used to love screen time. Then schools made Zoom mandatory all day long.*, WASH. POST (Sep. 4, 2020), <https://www.washingtonpost.com/technology/2020/09/04/screentime-school-distance/>.

32 Justin Lahart, *Covid Is Crushing Small Businesses. That's Bad News for American Innovation.*, WALL STREET J. <https://www.wsj.com/articles/covid-is-crushing-small-businesses-thats-bad-news-for-american-innovation-11602235804>.

Dissenting Statement

its investors.³³ The company seemed to guess that the FTC wouldn't do anything to materially impact their business. Sadly, for the public, they guessed right. Given the company's approach, efforts to hold Zoom accountable by regulators and enforcers in the U.S. and abroad will clearly need to continue.

Finally, the Federal Trade Commission has requested greater authority from Congress to protect Americans from abuse and misuse of personal data. But, actions like today's proposed settlement undermine these efforts. The agency must demonstrate that it is willing to use all of its existing tools to protect consumers and the market. Only then will the Commission be entrusted to take on more responsibilities.

It is critical that we restore the agency's credibility deficit when it comes to oversight of the digital economy. This does not stem from a lack of authority or resources or capabilities from our staff – it stems from the policy and enforcement approach of the Commission, and this needs to change.

For these reasons, I respectfully dissent.

DISSENTING STATEMENT OF COMMISSIONER REBECCA KELLY SLAUGHTER

Most weekday mornings, my two elementary-age children log on to school through Zoom. Their faces, voices, and occasional silliness are all captured in the Zoom classroom. I try not to dwell on what might occasionally float through in the background of their camera or microphone, but, like many families, we've had moments in our home where we are very much live. After my older kids settle in for class, my own workday begins in earnest and typically involves a series of confidential discussions often made possible through a Zoom meeting. My experience is not unique: Zoom expanded from 10 million daily users last December to over 300 million daily participants this spring. Zoom's overnight expansion from a modest video conferencing company to a company providing critical infrastructure for business, government, education, and social connection raises important questions for the Commission's obligations to protect consumer security and privacy.

³³ Zoom Video Communications, Inc., July 2020 Quarterly Report (Form 10-Q) (Sep. 3, 2020), <https://www.sec.gov/ix?doc=/Archives/edgar/data/1585521/000158552120000238/zm-20200731.htm>. When publicly traded firms do not disclose to their investors that they are facing a federal law enforcement inquiry, this suggests that they do not believe the inquiry is material to their financial or operational performance.

Dissenting Statement

Years before the global pandemic would make Zoom a household name, the company made decisions that threatened the security and privacy of its longstanding core business customers. Yet the Commission's proposed settlement provides no recourse for these paying customers. When Zoom's user base rapidly expanded, its failure to prioritize privacy and security suddenly posed a much more serious risk in terms of scope and scale. This proposed settlement, however, requires Zoom only to establish procedures designed to protect user *security* and fails to impose any requirements directly protecting user *privacy*. For a company offering services such as Zoom's, users must be able to trust that the company is committed to ensuring security and privacy alike.

Because the proposed resolution fails to require Zoom to address privacy as well as security, and because it fails to require Zoom to take any steps to correct the deception we charge it perpetrated on its paying clients, I respectfully dissent.

1. Zoom's Practices

As set forth in the Commission's complaint, Zoom engaged in a series of practices that undermined the security and privacy of its users. First, we allege Zoom made multiple misrepresentations about its use of encryption. As charged in the complaint, Zoom made false statements about its encryption being "end-to-end," the level of encryption that it offered, and the time it took to store recorded meetings in an encrypted server.¹

Zoom's problematic conduct was not limited to deception. The complaint charges that beginning in July 2018, Zoom secretly *and unfairly* deployed a web server, called the

"ZoomOpener," to circumvent certain Apple privacy and security safeguards enjoyed by Safari browser users. Because of these safeguards, Safari 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'?"² That is until, we allege, Zoom overrode this feature through its secret ZoomOpener, which bypassed the Safari safeguard to directly launch the Zoom App.³ The user was then automatically placed in the Zoom meeting, and, if the user had not changed her default video settings, her webcam was activated.⁴

In addition to these unfair and deceptive practices, which the Commission charged as law violations, there has been extensive public reporting on several other Zoom practices that raised serious privacy concerns. For example, Zoom business customers who subscribed to a service

1 See Complaint ¶¶ 16–33.

2 Complaint ¶ 35. If the user selected "Allow," the browser would connect the user to the Zoom meeting. *Id.* This safeguard was not specific to Zoom; Apple had designed its Safari browser to help defend its users from malicious actors and popular malware by requiring interaction with a dialogue box whenever any website or link attempted to launch an outside app. *Id.* at ¶ 34.

3 *Id.* at ¶ 36.

4 *Id.* at ¶ 37.

Dissenting Statement

called “LinkedIn Sales Navigator” had access to LinkedIn profile data about other users in a meeting—even when the other user wished to remain anonymous.⁵ Additionally, Security researchers found that Zoom-meeting video recordings saved on Zoom’s cloud servers had a predictable URL structure and were thus easy to find and view.⁶ And of course there was widespread coverage of “Zoom-bombing,” in which uninvited users crashed Zoom meetings.⁷ Zoom took steps to address these vulnerabilities after they surfaced by changing naming conventions, permanently removing the LinkedIn Sales Navigator app,⁸ and requiring meeting passwords as the default setting for more Zoom users,⁹ but these problems suggest Zoom’s approach to user privacy was fundamentally reactive rather than proactive.

2. *Lack of Privacy Protections*

Too often we treat data security and privacy as distinct concerns that can be separately preserved. In reality, protecting a consumer’s privacy and providing strong data security are closely intertwined, and when we solve only for one we fail to secure either. The Commission’s proposed order resolving its allegations against Zoom requires the company to establish an information-security program and submit to related independent third-party assessments. These provisions strive to improve data-security practices at the company and to send a signal to others regarding the baseline for adequate data-security considerations. Nowhere, however, is consumer privacy even mentioned in these provisions. This omission reflects a failure by the majority to understand that the reason customers care about security measures in products like Zoom is that they value their privacy.

Some might argue that sound data security practices should naturally guarantee consumer privacy. I disagree. Strong security is necessary for consumer privacy, but it does not guarantee its achievement. Zoom’s launch of its “ZoomOpener” to undermine the Apple Safari browser protections is an instructive example. Zoom prioritized maintaining its one-click functionality for users over privacy and security protections offered by Apple. The Commission’s proposed order tries to solve for this problem solely as a security issue and makes it difficult for Zoom to bypass third-party security features in the future. But the order does not address the core problem:

5 See Aaron Krolik and [Natasha Singer](#), *A Feature on Zoom Secretly Displayed Data From People’s LinkedIn Profiles*, N.Y. Times (Apr. 2, 2020), <https://www.nytimes.com/2020/04/02/technology/zoom-linkedin-data.html>. Zoom subsequently stated that it had disabled the feature.

6 See Paul Wagenseil, *Zoom security issues: Here’s everything that’s gone wrong (so far)*, Tom’s Guide (Nov. 3, 2020), <https://www.tomsguide.com/news/zoom-security-privacy-woes>.

7 See Jay Peters, *Zoom adds new security and privacy measures to prevent Zoombombing*, The Verge (Apr. 3, 2020), <https://www.theverge.com/2020/4/3/21207643/zoom-security-privacy-zoombombing-passwords-waiting-rooms-default>.

8 See Eric S. Yuan, *A Message To Our Users*, Zoom Blog (Apr. 1, 2020), <https://blog.zoom.us/a-message-to-our-users/>.

9 See Deepthi Jayarajan, *Enhanced Password Capabilities for Zoom Meetings, Webinars & Cloud Recordings*, Zoom Blog (Apr. 14, 2020), <https://blog.zoom.us/enhanced-password-capabilities-for-zoom-meetings-webinars-cloud-recordings/>.

Dissenting Statement

Zoom’s demonstrated inclination to prioritize some features, particularly ease of use, over privacy protections. Dumping Safari users automatically into a Zoom meeting, with their camera on, the first time they clicked on a link was not only a data-security failing—it was a privacy failing.

Similarly, we often discuss data encryption as a security issue, which of course it is, but we should simultaneously be recognizing it as a privacy issue. When customers choose encrypted communications, it is because they value their privacy in the content of their conversations. Treating encryption failures as a security-only issue fails to recognize the important privacy implications.

The FTC has approached privacy and security issues with related but distinct remedies: by imposing a comprehensive privacy program (as we did in *FTC v. Uber*) or by imposing a comprehensive information security program (as we did in *FTC v. Equifax*). This case provides a perfect example of a place where we ought to have required elements of both privacy and security programs. A more effective order would require Zoom to engage in a review of the risks to consumer *privacy* presented by its products and services, to implement procedures to routinely review such risks, and to build in privacy-risk mitigation before implementing any new or modified product, service, or practice. The Commission required this type of privacy-focused inquiry in the “Privacy Review Statement” provisions of its order in the *FTC v. Facebook* matter.¹⁰ Privacy-focused provisions such as these should either be added to relevant data-privacy orders as a separate privacy program or review, or the Commission’s information security programs should be modified to better integrate privacy and security.

When companies offer services with serious security and privacy implications for their users, the Commission must make sure that its orders address not only security but also privacy.

3. No Recourse for Customers

As of July 2019, Zoom had approximately 600,000 paying customers, and approximately 88% of those customers were small businesses with ten or fewer employees.¹¹ In securing these customers, the Commission charges that Zoom made express representations regarding its encryption offerings that were false. Yet, the proposed order does not require Zoom to take any steps to mitigate the impact of these statements we contend are false. Zoom is not required to offer redress, refunds, or even notice to its customers that material claims regarding the security of its services were false. This failure of the proposed settlement does a disservice to Zoom’s customers, and substantially limits the deterrence value of the case.

¹⁰ To be clear, I am not suggesting that Zoom’s conduct giving rise to this matter and Facebook’s order violations are equivalents. Nor do the companies share similar business models. But in terms of the importance of consumer privacy, hundreds of millions of users are entrusting Zoom with some of their most sensitive interactions, and they are doing so from their homes.

¹¹ Complaint ¶ 9.

Dissenting Statement

Finally, I join Commissioner Chopra's call for the Commission to engage in critical reflection to strengthen our enforcement efforts regarding technology across the board—from investigation to resolution.¹²

¹² Commissioner Chopra's dissenting statement sets forth an excellent list of *Recommendations and Corrective Actions* for the Commission to consider to improve the effectiveness of our enforcement efforts.

Analysis to Aid Public Comment

ANALYSIS OF CONSENT ORDER TO AID PUBLIC COMMENT

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

Analysis to Aid Public Comment

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.

Analysis to Aid Public Comment

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.

Complaint

IN THE MATTER OF

**PFIZER INC.,
UPJOHN INC.,
VIATRIS INC.,
MYLAN N.V.,
AND
UTAH ACQUISITION SUB INC.**

CONSENT ORDER, ETC. IN REGARD TO ALLEGED VIOLATIONS OF SECTION 5 OF THE FEDERAL
TRADE COMMISSION ACT AND SECTION 7 OF THE CLAYTON ACT

Docket No. C-4727; File No. 191 0182

Complaint, October 30, 2020 – Decision, January 25, 2021

This consent order addresses the combination of certain assets of Pfizer Inc. and Mylan N.V. to form Viatriis Inc. The complaint alleges that the Combination, if consummated, would violate Section 7 of the Clayton Act and Section 5 of the Federal Trade Commission Act by lessening current competition in the markets for: (1) amlodipine besylate/atorvastatin calcium tablets, (2) eplerenone tablets, (3) gatifloxacin ophthalmic solution, (4) medroxyprogesterone acetate injectable solution, (5) phenytoin chewable tablets, (6) prazosin hydrochloride (“HCl”) capsules, and (7) spironolactone hydrochlorothiazide (“HCTZ”) tablets in the United States. The complaint also alleges that the Combination would violate the aforementioned statutes by lessening future competition in the markets for: (1) levothyroxine sodium tablets, (2) sucralfate tablets, and (3) varenicline tartrate tablets. The consent order requires the parties to divest Upjohn’s generic drug rights and assets related to six products and Mylan’s rights and assets related to eplerenone tablets to Prasco, LLC. The consent order also requires prior Commission approval before Upjohn, Mylan, or Viatriis may gain an interest in or exercise control over any third party’s rights to (1) levothyroxine sodium tablets, (2) sucralfate tablets, and (3) varenicline tartrate tablets.

Participants

For the *Commission*: *Jasmine Y. Rosner, Danielle Sims and David von Nirschl.*

For the *Respondents*: *Harry T. Robins and Scott Stempel, Morgan, Lewis & Bockius LLP; Maggie D’Amico, Yonatan Even, and Christine Varney, Cravath, Swain & Moore LLP; Logan Breed, Chuck Loughlin, and Edith Ramirez, Hogan Lovells U.S. LLP.*

COMPLAINT

Pursuant to the Clayton Act and the Federal Trade Commission Act (“FTC Act”), and its authority thereunder, the Federal Trade Commission (“Commission”), having reason to believe that Respondent Pfizer Inc. proposes to combine certain of its assets and liabilities, including Respondent Upjohn Inc. and Respondent Utah Acquisition Sub Inc., with Respondent Mylan N.V. to form Respondent Viatriis Inc., all Respondents being corporations subject to the jurisdiction of the Commission, in violation of Section 5 of the FTC Act, as amended, 15 U.S.C. § 45, and that such combination, if consummated, would violate Section 7 of the Clayton Act, as amended, 15 U.S.C. § 18, and Section 5 of the FTC Act, as amended, 15 U.S.C. § 45, and it