192 3167

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Joseph J. Simons, Chairman**

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;

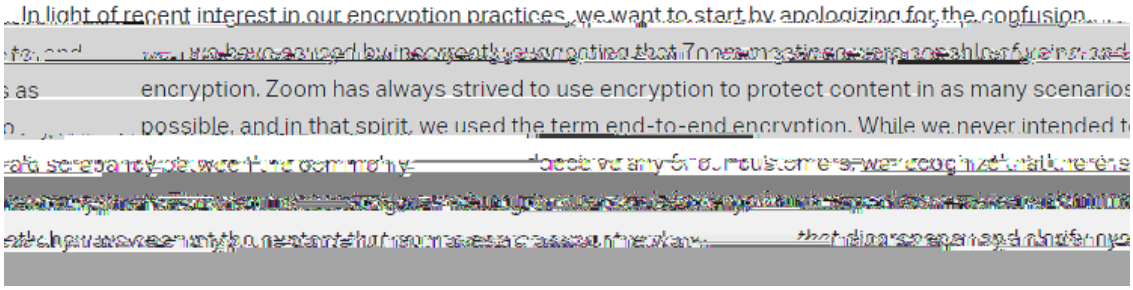
    b. Failed to test, audit, assess, or review its applications for security vulnerabilities at certain key points, such as prior to releasing software updates, including failing to ensure that its software is free from commonly known or reasonably foreseeable

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

24. In fact, Zoom did not provide end-to-end encryption for any Zoom Meeting that was conducted outside of Zoom's "Connecter" 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:



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

Zoom's Deceptive Claims Regarding Level of Encryption

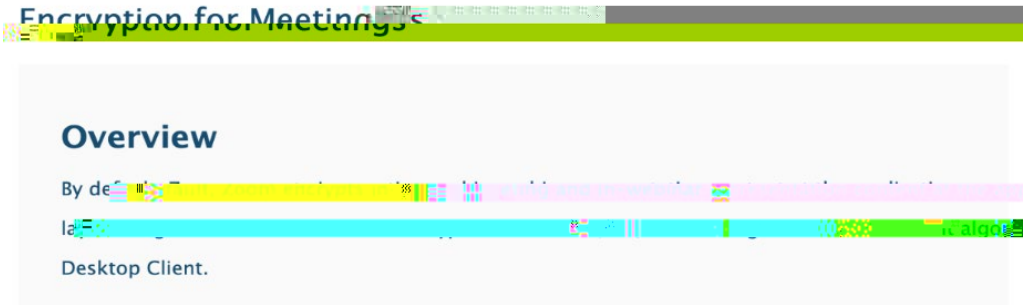
25. Encrypting communications with the Advanced Encryption Standard (AES) and a 256-bit encryption key can be an effective way to secure communications and prevent eavesdropping. The 256-bit encryption key refers to the length of the key needed to decrypt the communications. Generally speaking, a longer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



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.

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.

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 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

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

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

Violations of the FTC Act

65. The acts and practices of Zoom as alleged in this complaint constitute unfair or deceptive acts or pr