192 3167

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

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

In the Matter of

ZOOM VIDEO COMMUNICATIONS, INC., a corporation, d/b/a ZOOM.

DOCKET NO.

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.

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 "Connecter" 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.

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

    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.

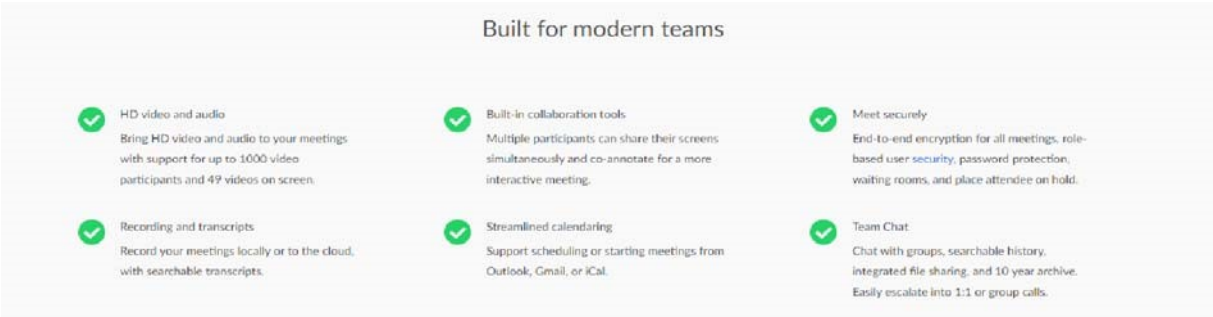
Zoom's Deceptive End-to-End Encryption Claims

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":



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."

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.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.