**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.**

**192** 3167

**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.

2.

**3**.

**4.**

**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**.

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**

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.

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.

**6.**

7.

**8.**

9.

10.

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)**.

**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.

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)**.

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**.

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.

**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.

2

11.

12.

13.

**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.

**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.**

b.

C.

**d.**

**e.**

f.

نیا

**Failed** to implement a training program **on** secure software development principles**;**

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**;**

**Failed to monitor service providers or other** contractors **who have access to Zoom's network;**

Failed to **secure** remote access **to** its networks and **systems** through multi**-**factor authentication or **similar** technology;

**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;

**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

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**."

**3**

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**.**

17.

**18.**

**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**.

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."

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**":

Built for modern teams

19.

HD video and audio

Bring HD video and audio to your meetings

with support for up to 1000 video

participants and 49 videos on screen

Built-in collaboration tools

Multiple participants can share their screens

simultaneously and co-annotate for **a** more

interactive meeting

Meet securely

End-to-end encryption for all meetings, role-

based user security, password protection

waiting **rooms**, and place attendee on hold.

Recording and transcripts

Record your meetings locally or to the cloud.

with searchable transcripts.

Streamlined calendaring

Support scheduling or starting meetings from

Outlook, Gmail, or Cal

Team Chat

Chat with groups, searchable history.

Integrated fie sharing, and 10 year archive.

Easily escalate into 1:1 or group calls.

**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**

**4**

20.

21.

22.

**23**.

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.

**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.

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."

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**.

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**.

5

24.

**25**.

26.

27*.*

**28**.

**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:

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

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.

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**")**.

**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)**.

**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**:

Protecting your Data

Communications are established using

256-bit TLS encryption and all shared

content can be encrypted using AES-

256 encryption.

6

**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**.

31.

**32**.

**33**.

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**

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")**.

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**.**"**

**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**.

7

**34**.

**35**.

36.

**37**.

**38.**

**39.**

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

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.

**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.

**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**.

**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."

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 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.

**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

**8**

**40.**

41.

**42**.

**43**.

**44.**

**45.**

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**).

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.

**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.

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**.

**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.

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.

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

9

46.

**47**.

**48.**

**49**.

50.

51.

security **policies** and practices **have** been **inconsistently** applied **across its systems**, and **it has** lacked an effective training program on secure software development principles.

**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.

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**.

**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

**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.

**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 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**.

**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**

10

52.

**53**.

**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**.

**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."**

54.

55.

56.

**VIOLATIONS OF THE FTC ACT**

**Count I**

**Deceptive Representation Regarding End-to-End Encryption**

**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.

**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**

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.

11

57.

**58.**

**59**.

60.

61.

**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**

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**.

**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**

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.

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

62.

63.

64.

**Count V**

**Deceptive Failure to** Disclose

**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**.

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**.

**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).

12

**65**.

**Violations** of **the FTC Act**

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**

**day** of

2020, **has**

issued **this Complaint against** Respondent.

SEAL:

**By the Commission**.

**13**

April J. Tabor **Acting** Secretary