



UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of the Secretary

January 19, 2021

Commenter Anonymous

Re: *In the Matter of Zoom Video Communications, Inc.*
FTC File No. 192 3167, FTC Docket No. C-4731

Dear Anonymous:

Thank you for your comment regarding the Federal Trade Commission's proposed consent agreement with Zoom Video Communications, Inc. ("Zoom").

The complaint in this matter alleges Zoom engaged in a number of deceptive and unfair practices. Specifically, the complaint alleges Zoom misrepresented its encryption practices—namely that it offered end-to-end encryption when it did not and that it offered a higher level of encryption than it provided. It also alleges the company represented it stored Zoom meeting recordings in an encrypted format in its secure cloud storage immediately after a meeting ended when, in fact, the recordings were kept unencrypted on Zoom's servers for up to sixty days before being transferred to secure cloud storage. Finally, the complaint alleges Zoom updated its application for Mac desktop computers in a deceptive and unfair way when it installed a piece of software that circumvented a Safari browser security feature without adequate notice or consent.

Your comment indicates the proposed settlement fails to address user privacy and security adequately. The Commission is committed to protecting consumer privacy and security. The proposed order is designed to address the misconduct alleged in the complaint, and help ensure consumers' security and privacy will be protected moving forward when they use Zoom. The proposed order prohibits the company from making a wide variety of security and privacy related misrepresentations. For example, Zoom is prohibited from making misrepresentations about its collection, maintenance, use, deletion, or disclosure of information from or about an individual; the extent to which it protects such information from unauthorized access; and how it maintains the privacy, security, confidentiality, or integrity of such information.

The proposed order also requires Zoom to implement a comprehensive information security program and institute safeguards to protect users' personal information via this program. For example, the program requires the company to implement specific security safeguards, such as performing a security review of all new software prior to release, conducting regular vulnerability scanning of its internal computer networks, and carrying out security training of its employees. The program also requires Zoom to implement specific privacy safeguards, such as implementing data deletion policies, procedures, and technical measures; limiting access to consumers' personal information to only those employees who need such access to perform their

jobs; using a default, randomized naming convention for saving recorded meetings; and implementing policies, procedures and technical measures to reduce the risk of third parties using users' log-in credentials without authorization. The company will be subject to independent, third-party assessments of its program. If Zoom fails to comply with any obligations under the proposed order, it could face substantial civil penalties.

The Commission is committed to protecting consumer privacy and security, and believes the proposed order offers substantial protections to Zoom users. For additional information on the settlement, including suggestions on how to video conference safely, please visit the Commission's consumer blog at <https://www.consumer.ftc.gov/blog/2020/11/settlement-requires-zoom-better-secure-your-personal-information>.

The Commission placed your comment on the public record pursuant to Rule 4.9(b)(6)(ii) of its Rules of Practice, 16 C.F.R. § 4.9(b)(6)(ii). The Commission has now determined the public interest would be served by issuing the Decision and Order in final form without any modifications. The final Decision and Order and other relevant materials are available from the Commission's website at <http://www.ftc.gov>. Thank you again for your comment.

By direction of the Commission, Commissioners Chopra and Slaughter dissenting.

April J. Tabor
Secretary



UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of the Secretary

January 19, 2021

Commenter Anonymous

Re: *In the Matter of Zoom Video Communications, Inc.*
FTC File No. 192 3167

Dear Anonymous:

Thank you for your comment regarding the Federal Trade Commission's proposed consent agreement with Zoom Video Communications, Inc. ("Zoom").

The complaint in this matter alleges Zoom engaged in a number of deceptive and unfair practices. Specifically, the complaint alleges Zoom misrepresented its encryption practices—namely that it offered end-to-end encryption when it did not and that it offered a higher level of encryption than it provided. It also alleges the company represented it stored Zoom meeting recordings in an encrypted format in its secure cloud storage immediately after a meeting ended when, in fact, the recordings were kept unencrypted on Zoom's servers for up to sixty days before being transferred to secure cloud storage. Finally, the complaint alleges Zoom updated its application for Mac desktop computers in a deceptive and unfair way when it installed a piece of software that circumvented a Safari browser security feature without adequate notice or consent.

Your comment indicates the proposed settlement fails to address user privacy and security adequately. The Commission is committed to protecting consumer privacy and security. The proposed order is designed to address the misconduct alleged in the complaint, and help ensure consumers' security and privacy will be protected moving forward when they use Zoom. The proposed order prohibits the company from making a wide variety of security and privacy related misrepresentations. For example, Zoom is prohibited from making misrepresentations about its collection, maintenance, use, deletion, or disclosure of information from or about an individual; the extent to which it protects such information from unauthorized access; and how it maintains the privacy, security, confidentiality, or integrity of such information.

The proposed order also requires Zoom to implement a comprehensive information security program and institute safeguards to protect users' personal information via this program. For example, the program requires the company to implement specific security safeguards, such as performing a security review of all new software prior to release, conducting regular vulnerability scanning of its internal computer networks, and carrying out security training of its employees. The program also requires Zoom to implement specific privacy safeguards, such as implementing data deletion policies, procedures, and technical measures; limiting access to consumers' personal information to only those employees who need such access to perform their

jobs; using a default, randomized naming convention for saving recorded meetings; and implementing policies, procedures and technical measures to reduce the risk of third parties using users' log-in credentials without authorization. The company will be subject to independent, third-party assessments of its program. If Zoom fails to comply with any obligations under the proposed order, it could face substantial civil penalties.

The Commission is committed to protecting consumer privacy and security, and believes the proposed order offers substantial protections to Zoom users. For additional information on the settlement, including suggestions on how to video conference safely, please visit the Commission's consumer blog at <https://www.consumer.ftc.gov/blog/2020/11/settlement-requires-zoom-better-secure-your-personal-information>.

The Commission placed your comment on the public record pursuant to Rule 4.9(b)(6)(ii) of its Rules of Practice, 16 C.F.R. § 4.9(b)(6)(ii). The Commission has now determined the public interest would be served by issuing the Decision and Order in final form without any modifications. The final Decision and Order and other relevant materials are available from the Commission's website at <http://www.ftc.gov>. Thank you again for your comment.

By direction of the Commission, Commissioners Chopra and Slaughter dissenting.

April J. Tabor
Secretary



Office of the Secretary

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

January 19, 2021

Commenter Barbara Bikman
State of Oregon

Re: *In the Matter of Zoom Video Communications, Inc.*
FTC File No. 192 3167, FTC Docket No. C-4731

Dear Ms. Bikman:

Thank you for your comment regarding the Federal Trade Commission's proposed consent agreement with Zoom Video Communications, Inc. ("Zoom").

The complaint in this matter alleges Zoom engaged in a number of deceptive and unfair practices. Specifically, the complaint alleges Zoom misrepresented its encryption practices—namely that it offered end-to-end encryption when it did not and that it offered a higher level of encryption than it provided. It also alleges the company represented it stored Zoom meeting recordings in an encrypted format in its secure cloud storage immediately after a meeting ended when, in fact, the recordings were kept unencrypted on Zoom's servers for up to sixty days before being transferred to secure cloud storage. Finally, the complaint alleges Zoom updated its application for Mac desktop computers in a deceptive and unfair way when it installed a piece of software that circumvented a Safari browser security feature without adequate notice or consent.

Your comment indicates the proposed settlement fails to address user privacy and security adequately, and specifically recommends the Commission consider the advice of the Electronic Privacy Information Center ("EPIC"). The Commission is committed to protecting consumer privacy and security, and the proposed settlement reflects expert input from a variety of sources. The Commission specifically considered EPIC's views, as expressed in their original July 2019 petition as well as their comment to the proposed order. You can review the Commission's response to EPIC's comment on www.ftc.gov.

The proposed order is designed to address the misconduct alleged in the complaint, and help ensure consumers' security and privacy will be protected moving forward when they use Zoom. The proposed order prohibits the company from making a wide variety of security and privacy related misrepresentations. For example, Zoom is prohibited from making misrepresentations about its collection, maintenance, use, deletion, or disclosure of information from or about an individual; the extent to which it protects such information from unauthorized access; and how it maintains the privacy, security, confidentiality, or integrity of such information.

The proposed order also requires Zoom to implement a comprehensive information security program and institute safeguards to protect users' personal information via this program. For example, the program requires the company to implement specific security safeguards, such as performing a security review of all new software prior to release, conducting regular vulnerability scanning of its internal computer networks, and carrying out security training of its employees. The program also requires Zoom to implement specific privacy safeguards, such as implementing data deletion policies, procedures, and technical measures; limiting access to consumers' personal information to only those employees who need such access to perform their job; using a default, randomized naming convention for saving recorded meetings; and implementing policies, procedures and technical measures to reduce the risk of third parties using users' log-in credentials without authorization. The company will be subject to independent, third-party assessments of its program. If Zoom fails to comply with any obligations under the proposed order, it could face substantial civil penalties.

The Commission is committed to protecting consumer privacy and security, and believes the proposed order offers substantial protections to Zoom users. For additional information on the settlement, including suggestions on how to video conference safely, please visit the Commission's consumer blog at <https://www.consumer.ftc.gov/blog/2020/11/settlement-requires-zoom-better-secure-your-personal-information>.

The Commission placed your comment on the public record pursuant to Rule 4.9(b)(6)(ii) of its Rules of Practice, 16 C.F.R. § 4.9(b)(6)(ii). The Commission has now determined the public interest would be served by issuing the Decision and Order in final form without any modifications. The final Decision and Order and other relevant materials are available from the Commission's website at <http://www.ftc.gov>. Thank you again for your comment.

By direction of the Commission, Commissioners Chopra and Slaughter dissenting.

April J. Tabor
Secretary



Office of the Secretary

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

January 19, 2021

Commenter Preston Bukaty
State of Colorado

Re: *In the Matter of Zoom Video Communications, Inc.*
FTC File No. 192 3167, FTC Docket No. C-4731

Dear Mr. Bukaty:

Thank you for your comment regarding the Federal Trade Commission's proposed consent agreement with Zoom Video Communications, Inc. ("Zoom").

The complaint in this matter alleges Zoom engaged in a number of deceptive and unfair practices. Specifically, the complaint alleges Zoom misrepresented its encryption practices—namely that it offered end-to-end encryption when it did not and that it offered a higher level of encryption than it provided. It also alleges the company represented it stored Zoom meeting recordings in an encrypted format in its secure cloud storage immediately after a meeting ended when, in fact, the recordings were kept unencrypted on Zoom's servers for up to sixty days before being transferred to secure cloud storage. Finally, the complaint alleges Zoom updated its application for Mac desktop computers in a deceptive and unfair way when it installed a piece of software that circumvented a Safari browser security feature without adequate notice or consent.

Your comment indicates the proposed settlement fails to address user privacy and security adequately. The Commission is committed to protecting consumer privacy and security. The proposed order is designed to address the misconduct alleged in the complaint, and help ensure consumers' security and privacy will be protected moving forward when they use Zoom. The proposed order prohibits the company from making a wide variety of security and privacy related misrepresentations. For example, Zoom is prohibited from making misrepresentations about its collection, maintenance, use, deletion, or disclosure of information from or about an individual; the extent to which it protects such information from unauthorized access; and how it maintains the privacy, security, confidentiality, or integrity of such information.

The proposed order also requires Zoom to implement a comprehensive information security program and institute specific safeguards to protect users' personal information via this program. For example, the program requires the company to implement specific security safeguards, such as performing a security review of all new software prior to release, conducting regular vulnerability scanning of its internal computer networks, and carrying out security training of its employees. The program also requires Zoom to implement specific privacy safeguards, such as implementing data deletion policies, procedures, and technical measures;

limiting access to consumers' personal information to only those employees who need such access to perform their job; using a default, randomized naming convention for saving recorded meetings; and implementing policies, procedures and technical measures to reduce the risk of third parties using users' log-in credentials without authorization. The company will be subject to independent, third-party assessments of its program. The Commission does not have the authority under current law to obtain civil penalties in cases, such as this one, for initial violations of the FTC Act. If Zoom fails to comply with any obligations under the proposed order, however, it could face substantial civil penalties.

The Commission is committed to protecting consumer privacy and security, and believes the proposed order offers substantial protections to Zoom users. For additional information on the settlement, including suggestions on how to video conference safely, please visit the Commission's consumer blog at <https://www.consumer.ftc.gov/blog/2020/11/settlement-requires-zoom-better-secure-your-personal-information>.

The Commission placed your comment on the public record pursuant to Rule 4.9(b)(6)(ii) of its Rules of Practice, 16 C.F.R. § 4.9(b)(6)(ii). The Commission has now determined the public interest would be served by issuing the Decision and Order in final form without any modifications. The final Decision and Order and other relevant materials are available from the Commission's website at <http://www.ftc.gov>. Thank you again for your comment.

By direction of the Commission, Commissioners Chopra and Slaughter dissenting.

April J. Tabor
Secretary



Office of the Secretary

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

January 19, 2021

Electronic Privacy Information Center
Center for Digital Democracy
Campaign for a Commercial-Free Childhood
Parent Coalition for Student Privacy
Consumer Federation of America

Re: *In the Matter of Zoom Video Communications, Inc.*
FTC File No. 192 3167, FTC Docket No. C-4731

Dear Electronic Privacy Information Center, et al.:

Thank you for your comment regarding the Federal Trade Commission's proposed consent agreement with Zoom Video Communications, Inc. ("Zoom").

The complaint in this matter alleges Zoom engaged in a number of deceptive and unfair practices. Specifically, the complaint alleges Zoom misrepresented its encryption practices—namely that it offered end-to-end encryption when it did not and that it offered a higher level of encryption than it provided. It also alleges the company represented it stored Zoom meeting recordings in an encrypted format in its secure cloud storage immediately after a meeting ended when, in fact, the recordings were kept unencrypted on its servers for up to sixty days before being transferred to secure cloud storage. Finally, the complaint alleges Zoom updated its application for Mac desktop computers in a deceptive and unfair way when it installed a piece of software that circumvented a Safari browser security feature without adequate notice or consent.

Your comment indicates you believe the proposed settlement fails to address consumer privacy adequately. In particular, you suggest in addition to the existing requirement to implement a comprehensive security program with biennial assessments by an independent, third-party assessor, the Commission should require Zoom to implement a comprehensive privacy program subject to biennial assessments by an independent third-party assessor, along with other relief that tracks the fair information practice principles. The proposed order is tailored to the allegations in the proposed complaint, which relate to the security of Zoom users' information. Nevertheless, the proposed order includes a number of privacy-related protections. For example, it prohibits the company from making misrepresentations about its collection, maintenance, use, deletion, or disclosure of information from or about an individual; the extent to which it protects such information from unauthorized access; and how it maintains the privacy, security, confidentiality, or integrity of such information. As part of the information security program, Zoom must implement a number of privacy-related safeguards, including implementing changes to its naming procedures for saving or storing recorded videoconference

meetings and developing data deletion policies and procedures. Public versions of these assessments can be requested through Freedom of Information Act (FOIA) requests, and Zoom, of course, is free to post the assessments on its website. These and other requirements serve to protect consumers' privacy as well as the security of their information and communications.

Your comment also suggests the proposed order should include redress for affected consumers. Notably, many consumers use Zoom's free services and would not be entitled to consumer redress. We believe the better course was to put in place broad injunctive relief that will protect consumers now, particularly while consumers rely heavily on Zoom to communicate during the pandemic.

Your comment also states the proposed order should include relief related to the collection of children's data because school districts across the country use Zoom for virtual learning. The Commission takes protection of children's data, and enforcement of the Children's Online Privacy Protection Act ("COPPA"), very seriously. The Commission has pursued more than 30 enforcement actions relating to COPPA violations, including a record-breaking penalty against Google and YouTube for \$170 million. Here, however, the complaint does not allege Zoom violated COPPA or otherwise engaged in any misconduct specifically related to children's data. Given this fact, we do not think it is good government to penalize companies for striving to meet consumers' needs to connect remotely during a global pandemic.

Finally, your comment suggests the Commission should engage in broader changes to its enforcement practices generally, not specific to this matter. The comment suggests the agency adopt a range of measures, including strengthening its orders, investigating firms comprehensively across the FTC's mission, diversifying its investigative teams to increase technical rigor, restating existing legal precedent into clear rules of the road to trigger monetary remedies for violations, demonstrating greater willingness to pursue administrative and federal court litigation, increasing cooperation with international, federal, and state partners, and determining whether third-party assessments are effective. Your comment also criticizes the approach to protecting consumer privacy and data security primarily through enforcement of Section 5 of the FTC Act (as opposed to rulemaking), and notes the Commission lacks statutory authority to obtain civil penalties for initial violations of Section 5. The Commission is committed to protecting consumer privacy and security. It staffs investigations, including the Zoom investigation, with technologists and others with similar expertise as appropriate. While many companies choose to settle their disputes, the Commission does not hesitate to pursue litigation when necessary to protect consumers. The Commission has asked Congress for additional tools, such as the ability to seek civil penalties for first-time privacy violations.¹

The Commission believes the proposed order offers substantial protections to Zoom users. It placed your comment on the public record pursuant to Rule 4.9(b)(6)(ii) of its Rules of Practice, 16 C.F.R. § 4.9(b)(6)(ii). The Commission has now determined the public interest would be served by issuing the Decision and Order in final form without any modifications.

¹ Please also see the Statement of Chairman Simons and Commissioners Phillips and Wilson, which addresses many of the points raised in your comment and Commissioner Chopra's dissenting statement. *See* https://www.ftc.gov/system/files/documents/public_statements/1577071/p065404dpipmajoritystatement.pdf

Letter to Commenters EPIC, et al.
Page 3

The final Decision and Order and other relevant materials are available from the Commission's website at <http://www.fcc.gov>. Thank you again for your comment.

By direction of the Commission, Commissioners Chopra and Slaughter dissenting.

April J. Tabor
Secretary



Office of the Secretary

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

January 19, 2021

Katie Moussouris
Chief Executive Officer
Luta Security

Re: *In the Matter of Zoom Video Communications, Inc.*
FTC File No. 192 3167, FTC Docket No. C-4731

Dear Ms. Moussouris

Thank you for your comment regarding the Federal Trade Commission's proposed consent agreement with Zoom Video Communications, Inc. ("Zoom").

The complaint in this matter alleges Zoom engaged in a number of deceptive and unfair practices. Specifically, the complaint alleges Zoom misrepresented its encryption practices—namely that it offered end-to-end encryption when it did not and that it offered a higher level of encryption than it provided. It also alleges the company represented it stored Zoom meeting recordings in an encrypted format in its secure cloud storage immediately after a meeting ended when, in fact, the recordings were kept unencrypted on Zoom's servers for up to sixty days before being transferred to secure cloud storage. Finally, the complaint alleges Zoom updated its application for Mac desktop computers in a deceptive and unfair way when it installed a piece of software that circumvented a Safari browser security feature without adequate notice or consent.

The Commission is committed to protecting consumer privacy and security. Your comment provides additional information about commercial bug bounty programs. Specifically, you point out several sources of friction in the vulnerability disclosure process, including required non-disclosure agreements and the lack of breadth in routing and escalating security incidents and breaches reported through the platform. Additionally, you highlight the importance of organizations like Zoom addressing relevant security issues and vulnerabilities within their own supply chain to support multiparty vulnerability coordination. We appreciate the insights you provide in the comment.

The proposed order is designed to address the misconduct alleged in the complaint, and help ensure consumers' security and privacy will be protected moving forward when they use Zoom. The proposed order prohibits the company from making a wide variety of security and privacy related misrepresentations. For example, it prohibits Zoom from making misrepresentations about its collection, maintenance, use, deletion, or disclosure of information from or about an individual; the extent to which it protects such information from unauthorized access; and how it maintains the privacy, security, confidentiality, or integrity of such

information. It also requires the company to implement a comprehensive information security program and institute specific safeguards via this program, such as performing security reviews of all new software prior to release, limiting access to consumers' personal information to those employees who need such access to perform their jobs, implementing data deletion practices, and carrying out security training of its employees. In addition, Zoom will be subject to independent, third-party assessments of its security program. If the company fails to comply with any obligations under the proposed order, it could face substantial civil penalties.

The Commission is committed to protecting consumer privacy and security, and believes the proposed order offers substantial protections to Zoom users. The Commission placed your comment on the public record pursuant to Rule 4.9(b)(6)(ii) of its Rules of Practice, 16 C.F.R. § 4.9(b)(6)(ii). The Commission has now determined the public interest would be served by issuing the Decision and Order in final form without any modifications. The final Decision and Order and other relevant materials are available from the Commission's website at <http://www.ftc.gov>. Thank you again for your comment.

By direction of the Commission, Commissioners Chopra and Slaughter dissenting.

April J. Tabor
Secretary



Office of the Secretary

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

January 19, 2021

Christine Bannan
Andi Wilson Thompson
Open Technology Institute
Washington, D.C.

Re: *In the Matter of Zoom Video Communications, Inc.*
FTC File No. 192 3167, FTC Docket No. C-4731

Dear Ms. Bannan and Ms. Wilson:

Thank you for your comment regarding the Federal Trade Commission's proposed consent agreement with Zoom Video Communications, Inc. ("Zoom").

The complaint in this matter alleges Zoom engaged in a number of deceptive and unfair practices. Specifically, the complaint alleges Zoom misrepresented its encryption practices—namely that it offered end-to-end encryption when it did not and that it offered a higher level of encryption than it provided. It also alleges Zoom represented that it stored Zoom meeting recordings in an encrypted format in its secure cloud storage immediately after a meeting ended when, in fact, the recordings were kept unencrypted on Zoom's servers for up to sixty days before being transferred to secure cloud storage. Please note that while the complaint alleges Zoom used a lower level of encryption than promised, the complaint did not allege Zoom meetings were entirely unencrypted – an apparent concern raised in your comment. Zoom's default setting encrypted meetings with the same level of encryption the National Security Agency has reported may be used to secure "SECRET" communications. Finally, the complaint alleges Zoom updated its application for Mac desktop computers in a deceptive and unfair way when it installed a piece of software that circumvented a Safari browser security feature without adequate notice or consent.

Your comment indicates you believe the proposed settlement fails to address consumer privacy adequately. In particular, you suggest in addition to the existing requirement to implement a comprehensive security program with biennial assessments by an independent, third-party assessor, the Commission should require Zoom to implement a comprehensive privacy program. The proposed order is tailored to the allegations in the proposed complaint, which relate to the security of Zoom users' information. Nevertheless, the proposed order includes a number of privacy-related protections. For example, it prohibits Zoom from making misrepresentations about its collection, maintenance, use, deletion, or disclosure of information from or about an individual; the extent to which the company protects such information from

unauthorized access; and how it maintains the privacy, security, confidentiality, or integrity of such information. As part of the information security program, Zoom must implement a number of privacy-related safeguards, including implementing changes to its naming procedures for saving or storing recorded videoconference meetings and developing data deletion policies and procedures. These and other requirements serve to protect consumers' privacy as well as the security of their information and communications.

Your comment also suggests the proposed order should include consumer notice and a remedy for affected consumers. Notably, many consumers use Zoom's free services. These consumers would not be entitled to consumer redress or need to cancel their service agreements with Zoom. Additionally, many of the company's customers are already aware from press reports that Zoom was providing a lower level of encryption than it had promised. Further, the company announced in April 2020 that it was securing its meetings, in part, with AES 256-bit encryption, and the company announced in October 2020 that it would begin offering end-to-end encryption for all meetings. As opposed to engaging in protracted litigation to seek such additional relief, we believe the better course is to put in place broad injunctive relief that will protect all consumers now, particularly while consumers rely heavily on Zoom to communicate during the pandemic.

Your comment also states the FTC should examine the effectiveness of third-party assessments in detecting and preventing future misconduct, not specific to this matter. In recent orders, including the proposed order in this case, the Commission has implemented additional requirements on third-party assessors than what was in place at the time of the Commission's 2012 order with Facebook, Inc. For example, the proposed order specifically requires assessors to identify evidence to support their conclusions, not depend on management assertions, retain documents related to the assessment, and provide them to the Commission when asked. The Commission also has authority to approve and re-approve assessors every two years. *See* Andrew Smith, Director of the Bureau of Consumer Protection, *New and improved FTC data security orders: Better guidance for companies, better protection for consumers* (Jan. 6, 2020), available at <https://www.ftc.gov/news-events/blogs/business-blog/2020/01/new-improved-ftc-data-security-orders-better-guidance>. In addition to the third party assessments, our orders also include provisions that enable the Commission to monitor compliance with its orders directly.

Finally, your comment supports broader changes to the Commission's enforcement practices generally, not specific to this matter, as expressed in Commissioner Chopra's dissenting statement. The Commission is committed to protecting consumer privacy and security, and has asked Congress for additional tools to protect consumer privacy and security, such as the ability to seek civil penalties for first-time privacy violations. Please see the Statement of Chairman Simons and Commissioners Phillips and Wilson, which addresses many of the points raised in Commissioner Chopra's dissenting statement. *See* https://www.ftc.gov/system/files/documents/public_statements/1582922/1923167zoommajoritystatement.pdf.

The Commission believes the proposed order offers substantial protections to Zoom users. The Commission placed your comment on the public record pursuant to Rule 4.9(b)(6)(ii) of its Rules of Practice, 16 C.F.R. § 4.9(b)(6)(ii). The Commission has now determined the

public interest would be served by issuing the Decision and Order in final form without any modifications. The final Decision and Order and other relevant materials are available from the Commission's website at <http://www.ftc.gov>. Thank you again for your comment.

By direction of the Commission, Commissioners Chopra and Slaughter dissenting.

April J. Tabor
Secretary



UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of the Secretary

January 19, 2021

Commenter Melinda Place

Re: *In the Matter of Zoom Video Communications, Inc.*
FTC File No. 192 3167, FTC Docket No. C-4731

Dear Ms. Place:

Thank you for your comment regarding the Federal Trade Commission's proposed consent agreement with Zoom Video Communications, Inc. ("Zoom").

The complaint in this matter alleges Zoom engaged in a number of deceptive and unfair practices. Specifically, the complaint alleges Zoom misrepresented its encryption practices—namely that it offered end-to-end encryption when it did not and that it offered a higher level of encryption than it provided. It also alleges Zoom represented that it stored Zoom meeting recordings in an encrypted format in its secure cloud storage immediately after a meeting ended when, in fact, the recordings were kept unencrypted on Zoom's servers for up to sixty days before being transferred to secure cloud storage. Please note that while the complaint alleges Zoom used a lower level of encryption than promised, the complaint did not allege Zoom meetings were entirely unencrypted – a concern raised in your comment. Zoom's default setting encrypted meetings with the same level of encryption the National Security Agency has reported may be used to secure "SECRET" communications. Finally, the complaint alleges Zoom updated its application for Mac desktop computers in a deceptive and unfair way when it installed a piece of software that circumvented a Safari browser security feature without adequate notice or consent.

The proposed order is designed to address this misconduct, and help ensure consumers' security and privacy will be protected moving forward when they use Zoom. The proposed order prohibits Zoom from making a wide variety of security and privacy related misrepresentations. It also requires Zoom to implement a comprehensive information security program and institute specific safeguards via this program, such as performing a security review of all new software, carrying out security training of its employees, and conducting vulnerability scans on at least a quarterly basis. In addition, Zoom will be subject to independent, third-party assessments of its security program.

With respect to your suggestion that the Commission should penalize Zoom with a fine or other monetary penalty, the Commission does not have the authority under current law to obtain civil penalties in cases, such as this one, for initial violations of the FTC Act. If Zoom fails to

comply with any obligations under the proposed order, however, it could face substantial civil penalties.

The Commission placed your comment on the public record pursuant to Rule 4.9(b)(6)(ii) of its Rules of Practice, 16 C.F.R. § 4.9(b)(6)(ii). The Commission has now determined the public interest would be served by issuing the Decision and Order in final form without any modifications. The final Decision and Order and other relevant materials are available from the Commission's website at <http://www.ftc.gov>. Thank you again for your comment.

By direction of the Commission, Commissioners Chopra and Slaughter dissenting.

April J. Tabor
Secretary



Office of the Secretary

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

January 19, 2021

Commenter C. Warren Pope
State of North Carolina

Re: *In the Matter of Zoom Video Communications, Inc.*
FTC File No. 192 3167, FTC Docket No. C-4731

Dear Mr. Pope:

Thank you for your comment regarding the Federal Trade Commission's proposed consent agreement with Zoom Video Communications, Inc. ("Zoom").

The complaint in this matter alleges Zoom engaged in a number of deceptive and unfair practices. Specifically, the complaint alleges Zoom misrepresented its encryption practices—namely that it offered end-to-end encryption when it did not and that it offered a higher level of encryption than it provided. It also alleges the company represented it stored Zoom meeting recordings in an encrypted format in its secure cloud storage immediately after a meeting ended when, in fact, the recordings were kept unencrypted on Zoom's servers for up to sixty days before being transferred to secure cloud storage. Finally, the complaint alleges Zoom updated its application for Mac desktop computers in a deceptive and unfair way when it installed a piece of software that circumvented a Safari browser security feature without adequate notice or consent.

Your comment indicates the proposed settlement fails to address user privacy adequately. In addition to addressing security issues, the order does explicitly protect consumer privacy. For example, Zoom is prohibited from making misrepresentations about its collection, maintenance, use, deletion, or disclosure of information from or about an individual; the extent to which it protects such information from unauthorized access; and how it maintains the privacy, confidentiality, or integrity of such information.

The proposed order also requires specific privacy safeguards. For example, it requires Zoom to implement data deletion policies, procedures, and technical measures; limit access to consumers' personal information to only those employees who need such access to perform their job; use a default, randomized naming convention for saving recorded meetings; and implement policies, procedures and technical measures to reduce the risk of third parties using users' log-in credentials without authorization. The company will be subject to independent, third-party assessments to ensure that it is meeting these requirements. If Zoom fails to comply with any obligations under the proposed order, it could face substantial civil penalties.

The Commission is committed to protecting consumer privacy and security, and believes the proposed order offers substantial protections to Zoom users. For additional information on the settlement, including suggestions on how to video conference safely, please visit the Commission's consumer blog at <https://www.consumer.ftc.gov/blog/2020/11/settlement-requires-zoom-better-secure-your-personal-information>.

The Commission placed your comment on the public record pursuant to Rule 4.9(b)(6)(ii) of its Rules of Practice, 16 C.F.R. § 4.9(b)(6)(ii). The Commission has now determined that the public interest would be served by issuing the Decision and Order in final form without any modifications. The final Decision and Order and other relevant materials are available from the Commission's website at <http://www.ftc.gov>. Thank you again for your comment.

By direction of the Commission, Acting Chairwoman Slaughter and Commissioner Chopra dissenting.

April J. Tabor
Secretary



Office of the Secretary

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

January 19, 2021

Commenter Lindsey Stidam

Re: *In the Matter of Zoom Video Communications, Inc.*
FTC File No. 192 3167, FTC Docket No. C-4731

Dear Ms. Stidam:

Thank you for your comment regarding the Federal Trade Commission's proposed consent agreement with Zoom Video Communications, Inc. ("Zoom").

The complaint in this matter alleges Zoom engaged in a number of deceptive and unfair practices. Specifically, the complaint alleges Zoom misrepresented its encryption practices—namely that it offered end-to-end encryption when it did not and that it offered a higher level of encryption than it provided. It also alleges the company represented it stored Zoom meeting recordings in an encrypted format in its secure cloud storage immediately after a meeting ended when, in fact, the recordings were kept unencrypted on Zoom's servers for up to sixty days before being transferred to secure cloud storage. Finally, the complaint alleges Zoom updated its application for Mac desktop computers in a deceptive and unfair way when it installed a piece of software that circumvented a Safari browser security feature without adequate notice or consent.

The Commission is committed to protecting consumer privacy and security. You indicate you are a student and may need to use Zoom if a teacher or school district requires it. You state that you felt uncomfortable using Zoom while knowing of the alleged misconduct, and now the order makes you feel more at ease about the company's practices going forward. As you wrote, the proposed order is designed to address the misconduct alleged in the complaint, and help ensure consumers' security and privacy will be protected moving forward when they use Zoom. The proposed order prohibits the company from making a wide variety of security and privacy related misrepresentations. For example, Zoom is prohibited from making misrepresentations about its collection, maintenance, use, deletion, or disclosure of information from or about an individual; the extent to which it protects such information from unauthorized access; and how it maintains the privacy, security, confidentiality, or integrity of such information.

The order also requires the company to implement a comprehensive information security program and institute specific safeguards via this program, such as a performing a security review of all new software prior to release, limiting access to consumers' personal information to only those employees who need such access to perform their jobs, implementing data deletion practices, and carrying out security training of its employees. In addition, Zoom will be subject

to independent, third-party assessments of its security program. If the company fails to comply with any obligations under the proposed order, it could face substantial civil penalties.

The Commission is committed to protecting consumer privacy and security, and believes the proposed order offers substantial protections to Zoom users. For additional information on the settlement, including suggestions on how to safely video conference, please visit the Commission's consumer blog at <https://www.consumer.ftc.gov/blog/2020/11/settlement-requires-zoom-better-secure-your-personal-information>.

The Commission placed your comment on the public record pursuant to Rule 4.9(b)(6)(ii) of its Rules of Practice, 16 C.F.R. § 4.9(b)(6)(ii). The Commission has now determined that the public interest would be served by issuing the Decision and Order in final form without any modifications. The final Decision and Order and other relevant materials are available from the Commission's website at <http://www.ftc.gov>. Thank you again for your comment.

By direction of the Commission, Commissioners Chopra and Slaughter dissenting.

April J. Tabor
Secretary



UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of the Secretary

January 19, 2021

Commenter Maria Zunun

Re: *In the Matter of Zoom Video Communications, Inc.*
FTC File No. 192 3167, FTC Docket No. C-4731

Dear Ms. Zunun:

Thank you for your comment regarding the Federal Trade Commission's proposed consent agreement with Zoom Video Communications, Inc. ("Zoom").

The complaint in this matter alleges Zoom engaged in a number of deceptive and unfair practices. Specifically, the complaint alleges Zoom misrepresented its encryption practices—namely that it offered end-to-end encryption when it did not and that it offered a higher level of encryption than it provided. It also alleges the company represented it stored Zoom meeting recordings in an encrypted format in its secure cloud storage immediately after a meeting ended when, in fact, the recordings were kept unencrypted on Zoom's servers for up to sixty days before being transferred to secure cloud storage. Finally, the complaint alleges Zoom updated its application for Mac desktop computers in a deceptive and unfair way when it installed a piece of software that circumvented a Safari browser security feature without adequate notice or consent.

The Commission is committed to protecting consumer privacy and security. You noted the proposed complaint is a great step in protecting Zoom users and their security. Indeed, the proposed order is designed to address the misconduct alleged in the complaint, and help ensure consumers' security and privacy will be protected moving forward when they use Zoom. The proposed order prohibits the company from making a wide variety of security and privacy related misrepresentations. For example, Zoom is prohibited from making misrepresentations about its collection, maintenance, use, deletion, or disclosure of information from or about an individual; the extent to which it protects such information from unauthorized access; and how it maintains the privacy, security, confidentiality, or integrity of such information. It also requires Zoom to implement a comprehensive information security program and institute specific safeguards via this program, such as a performing a security review of all new software prior to release, limiting access to consumers' personal information to only those employees who need such access to perform their job, implementing data deletion practices, and carrying out security training of its employees. In addition, Zoom will be subject to independent, third-party assessments of its security program. If the company fails to comply with any obligations under the proposed order, it could face substantial civil penalties.

The Commission is committed to protecting consumer privacy and security, and believes the proposed order offers substantial protections to Zoom users. For additional information on the settlement, including suggestions on how to video conference safely, please visit the Commission's consumer blog at <https://www.consumer.ftc.gov/blog/2020/11/settlement-requires-zoom-better-secure-your-personal-information>.

The Commission placed your comment on the public record pursuant to Rule 4.9(b)(6)(ii) of its Rules of Practice, 16 C.F.R. § 4.9(b)(6)(ii). The Commission has now determined that the public interest would be served by issuing the Decision and Order in final form without any modifications. The final Decision and Order and other relevant materials are available from the Commission's website at <http://www.ftc.gov>. Thank you again for your comment.

By direction of the Commission, Commissioners Chopra and Slaughter dissenting.

April J. Tabor
Secretary