GUTRIDE SAFIER LLP
ADAM J. GUTRIDE (State Bar No. 181446)
SETH A. SAFIER (State Bar No. 197427)
MARIE A. MCCRARY (State Bar No. 262670)
100 Pine Street, Suite 1250
San Francisco, CA 94111
Telephone: (415) 271-6469
Facsimile: (415) 449-6469

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT FOR THE

NORTHERN DISTRICT OF CALIFORNIA

ROBERT LAWTON, as an individual, on behalf of himself, the general public and those similarly situated, Plaintiff, v. ZOOM VIDEO COMMUNICATIONS, INC., Defendant.	CASE NO. **CLASS ACTION COMPLAINT FOR VIOLATION OF THE CALIFORNIA CONSUMERS LEGAL REMEDIES ACT; FALSE ADVERTISING; FRAUD, DECEIT, AND/OR MISREPRESENTATION; UNFAIR BUSINESS PRACTICES; AND VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT** JURY TRIAL DEMANDED

INTRODUCTION

1. Plaintiff Robert Lawton, by and through his counsel, brings this class action against Defendant Zoom Communications, Inc., to seek redress for Defendant's deceptive practices relating to its video and audio conferencing software.

2. Zoom provides an overwhelmingly popular online platform for video and audio conferencing, collaboration, chat, and webinars. Zoom promises customers that its products allow them to "meet securely" though "end-to-end encryption for all meetings, role-based user security, password protection, waiting rooms, and place attendee on hold." Zoom's chief product is "Zoom Meetings."

3. Zoom consistently violates its duty to its over 200 million users to implement and maintain reasonable security practices, fails to disclose known security risks, and affirmatively misleads consumers about the security benefits of its product.

4. In particular, Zoom collects private information about its users and discloses this information to Facebook, LinkedIn, other users, and other third parties. Zoom intentionally omits this fact from its privacy policy and misleads reasonable consumers to believe that the information they share in Zoom meetings is private.

5. Further, Zoom claims to offer users the privacy and protection of end-to-end encryption, the most secure form of internet communication. In reality, Zoom does not offer end-to-end encryption, and its software cannot even support such security measures. Instead, Zoom accesses private information that users share on the Zoom network.

6. Zoom has also failed to disclose or remedy known vulnerabilities that allow hackers and other websites to forcibly access a user's webcam, join a user to a Zoom call without his or her permission, and access recordings of Zoom meetings.

7. Plaintiff brings this class action on behalf of all similarly situated consumers who used and/or purchased Zoom's product believing that the product was secure and that their information was safe.

8. Plaintiff seeks injunctive relief and restitution against Zoom for false and misleading advertising in violation of Business and Professions Code Section 17200, *et seq.*,

Business and Professions Code Section 17500, *et seq.*, and Civil Code Section 1750, *et seq.*, and for violating the Consumer Privacy Act. Zoom made and continues to make these false and misleading statements in its advertising of the product. Zoom also continues to invade the privacy of innocent users and leave them vulnerable to security threats. Compliance with remedial statutes like those underlying this lawsuit will benefit Plaintiff, the putative class, consumers, and the general public.

PARTIES

9. Robert Lawton ("Plaintiff") is, and at all times alleged in this Class Action Complaint was, an individual and a resident San Francisco, California.

10. Defendant Zoom Video Communications, Inc. ("Defendant" or "Zoom") is a Delaware corporation headquartered in San Jose, California. Defendant maintains its principal place of business at 55 Almaden Blvd., 6th Floor, San Jose, CA 95113. Defendant directly and through its agents, has substantial contacts with and receives substantial benefits and income from and through the United States and/or State of California. Defendant is one of the owners, manufacturers, and distributors of the software product, and is one of the companies that created and/or authorized the false, misleading, and deceptive claims on the product website.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. Section 1332(d)(2)(A) because: (i) there are 100 or more class members, and (ii) there is an aggregate amount in controversy exceeding $5,000,000, exclusive of interest and costs.

12. This Court has supplemental jurisdiction over any state law claims pursuant to 28 U.S.C. Section 1367.

13. The injuries, damages and/or harm upon which this action is based, occurred or arose out of activities engaged in by Defendant within, affecting, and emanating from, the State of California. Defendant regularly conducts and/or solicits business in, engages in other persistent courses of conduct in, and/or derives substantial revenue from products provided to persons in the State of California. Defendant has engaged, and continues to engage, in substantial and

continuous business practices in the State of California.

14. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claims occurred in the state of California, including within this District.

15. In accordance with California Civil Code Section 1780(d), Plaintiff concurrently files herewith a declaration establishing that he downloaded and used the Zoom Meetings software in San Francisco, California. (Plaintiff's declaration is attached hereto as Exhibit A.)

16. Plaintiff accordingly alleges that jurisdiction and venue are proper in this Court.

SUBSTANTIVE ALLEGATIONS

17. Defendant provides an online platform for video and audio conferencing, collaboration, chat, and webinars. Defendant promises customers that its products allow them to "meet securely" though "end-to-end encryption for all meetings, role-based user security, password protection, waiting rooms, and place attendee on hold." Zoom's chief product is "Zoom Meetings" (the "Product"). Zoom has emerged as a fundamental online utility, with 200 million daily users — including family members gathering to celebrate holidays, teachers leading online classes for students and members of Alcoholics Anonymous holding meetings. (Zoom Blog, A Message to Our Users, https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/ (last visited April 3, 2020).)

18. Zoom operates a "freemium" business model: users can sign up for a Basic Plan, which allows them to host groups of up to 100 people for up to 40 minutes at a time at no charge, but users must pay $14.99 per month or more for extra features, like bigger groups and administrative controls, with a Pro, Business or Enterprise Plan. Zoom users can access the Product through mobile applications, as well as through desktop computers and telephones.

19. Zoom has profited off of users' desire to stay connected professionally and personally during the global pandemic and the accompanying stay-at-home orders. Zoom's stock price has increased from $62 in October of 2019 to as high as $159.56 in March of 2020.

Zoom Shares Private User Information with Facebook

20. Each time a user downloaded or opened the Zoom iOS app on a mobile device ("App"), Zoom shared the user's personal and private information with Facebook without obtaining customers' consent—or even notifying customers of this practice. In particular, Zoom would notify Facebook that the user had opened the App; provide details on the user's device such as the model, time zone, and city he or she was connecting from; and share a unique advertiser identifier created by the user's device which companies can use to target a user with advertisements. Each of these device-specific identifiers can be linked to the individual identity of the Zoom customer. Zoom provided Facebook with this private information even if the user did not have a Facebook account. Upon information and belief, Zoom provides customer personally identifiable information ("PII") to other unauthorized third parties for use in targeted advertising

21. The process by which this occurred was described in detail in a March 26, 2020 Motherboard article. (Joseph Cox, Zoom iOS App Sends Data to Facebook Even if You Don't Have a Facebook Account, MOTHERBOARD, available at https://www.vice.com/en_us/article/k7e599/zoom-ios-app-sends-data-to-facebook-even-if-you-dont-have-a-facebook-account (last visited April 3, 2020).) Upon downloading and opening the App, Zoom would connect to Facebook's Graph API. The Graph API is the main way that app developers get data in or out of Facebook. The Zoom app would notify Facebook when the user opened the App; details on the user's device, such as the model, time zone and city from which they were connecting, which phone carrier they were using; and a unique advertiser identifier created by the user's device which companies can use to target a user with advertisements. The disclosure of the unique advertiser identifier (also known as an "IDFA," or, "Identifier for Advertisers") are unique, alphanumeric strings that are used to identify an individual device—and the individual who uses that device—to track and profile the user.

22. Advertisers use the IDFA to track data so that they can deliver customized advertising. The IDFA is used for tracking and identifying a user, allowing whoever is tracking it to identify when users interact with mobile advertising and whether specific users click advertisements. An IDFA is similar to a cookie in that it allows advertisers to know that a specific iPhone

user is looking at a specific publication so that it can serve an ad targeting that user. Key digital privacy and consumer groups have described why and how an identifier like an IDFA facilitates targeted advertising and is not "anonymous" at all, even though the IDFA itself does not contain the user's name.

23. Other information shared by Zoom can also allow users to be identified individually. Details about the type of device (e.g., iPhone or iPad), details about its software (iOS), its network carrier (e.g., Spring, T-Mobile, AT&T), and the location of the user, when taken together, provide a high level of detail about the user. In combination with the IDFA, the information shared is extremely detailed and can be used to identify the user personally.

24. Advertisers use this information to learn more about users, including when and how they use the Zoom platform, along with their behaviors, demographics, and preferences, so that they can serve them with tailored and targeted advertising. Thereafter, anyone with access to the IDFA can track the effectiveness of those advertisements after the user sees them.

25. This information has tremendous economic value. Moreover, the disclosure of this identifying information makes people more vulnerable to voter fraud, medical fraud, phishing, and other identity-based harms. But most importantly, the ability to de-annonymize and analyze user data allows parties to personally and psychologically target Zoom's customers with great precision.

26. The information shared by Zoom allows Facebook and any other recipient to spy on Zoom's customers and deliver targeted advertisements to them as they browse the internet, as well as to determine the effectiveness of the advertisements.

27. Zoom's data-sharing activity was not visible to the user, who simply saw the Zoom App interface, and Zoom users had no reason to expect that Zoom would transmit their PII to Facebook, a completely unrelated social networking company, or any other undisclosed third party, to be used to track and target them for advertising. Moreover, Zoom's privacy policy stated that Google Ads and Google Analytics "automatically collect some information about you when you use our products;" however, Zoom's privacy policy fails to mention that it collects and shares any information with Facebook. Since users could not detect this activity from the App itself, and

Zoom does not allow them to monitor whether it is sharing their PII, users of Zoom have no reasonable way of knowing whether, when they open the Zoom App, their PII will be safeguarded or disclosed without their consent. Zoom never received consent to transfer user data to Facebook.

28. Consumers are interested in how much of their personal information is being shared with third-party advertisers. Had Plaintiff and the class known that Zoom shared PII with Facebook, they would not have purchased or used Zoom and would have opted to use a different product that did not share their private information with Facebook.

29. Zoom admitted it was violating users' privacy. In particular, Zoom released a statement saying "we were recently made aware that the Facebook SDK was collecting unnecessary device data." (Zoom Blog, *Zoom's Use of Facebook's SDK in iOS Client*, https://blog.zoom.us/wordpress/2020/03/27/zoom-use-of-facebook-sdk-in-ios-client/ (last visited April 3, 2020).) Zoom further stated that "[u]sers will need to update to the latest version of our application once it becomes available in order for these changes to take hold, and we encourage them to do so. We sincerely apologize for this oversight, and remain firmly committed to the protection of our users' data." (Id.)

30. On March 27, 2020, Zoom released a new version of the App, which purports to no longer send unauthorized PII of its users to Facebook. However, even assuming this updated version works as described by Zoom, the harm to Plaintiff and the Class Members has been done and continues. Zoom appears to have taken no action to block any of the prior versions of the Zoom App from operating. Thus, unless users affirmatively update their Zoom App, they likely will continue to unknowingly send unauthorized personal information to Facebook, and perhaps other third parties. Zoom could have forced all iOS users to update to the new Zoom App to continue using Zoom but appears to have chosen not to.

31. Moreover, the ostensibly corrected Zoom App does nothing to remedy the unauthorized disclosures made by Zoom to date. Zoom has not ensured that Facebook (or anyone else, including others with whom Facebook has shared this personal information) has deleted all the PII that it received from Zoom without adequate notice or authorization by Zoom's users. Finally,

Zoom has not taken any actions to compensate its users for its failure to properly safeguard their PII in violation of their right of privacy and California's consumer protection laws.

Zoom Shares Private Linkedin Information With Users

32. A data-mining feature on the Product allowed participants to access LinkedIn profile data about other users who signed into the meeting— without asking for their permission during the meeting or even notifying them that their LinkedIn data was available to other users.

33. The process by which this occurred was described in an April 2, 2020 New York Times article. (Aaron Krolik and Natasha Singer, "A Feature on Zoom Secretly Displayed Data From People's LinkedIn Profiles," April 2, 2020, available at https://nyti.ms/343pByJ (last accessed April 3, 2020).) The data-mining feature was available to Zoom users who subscribed to a LinkedIn service for sales prospecting, called LinkedIn Sales Navigator. Once a Zoom user enabled the feature, that person could view LinkedIn profile data about users — like locations, employer names and job titles — for people in the Zoom meeting by clicking on a LinkedIn icon next to their names. Even when a user signed into the Zoom meeting under a pseudonym, the data-mining tool matched the "anonymous" user with her LinkedIn profile, thereby overriding her efforts to keep it private. Zoom automatically sent participants' PII to its LinkedIn data-mining tool even when no one in a meeting had activated it.

34. Again, Zoom's LinkedIn data-mining activity was not visible to the user, who simply saw the Zoom App interface, and Zoom users had no reason to expect that Zoom would transmit their LinkedIn profile data. Zoom's privacy policy fails to mention that it could display meeting participants' LinkedIn data to Zoom or other users — or that it might communicate the names and email addresses of participants in private Zoom meetings to LinkedIn. In fact, user instructions on Zoom suggested just the opposite, i.e., that meeting attendees may control who sees their real names.

Zoom Falsely Advertises that its Software is Secure

35. Zoom claims to implement end-to-end encryption, widely understood as the most secure, private form of internet communication, protecting conversations from all outside parties. Consumers are interested in the type of security offered by companies like Zoom and rely on

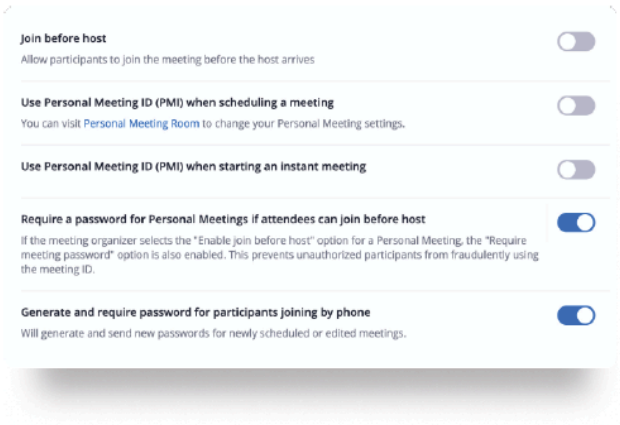
Zoom's advertising statements to determine which product to use and purchase. However, this is false, deceptive, and misleading because Zoom does not use end-to-end encryption and instead it offers what is usually called transport encryption, which, as explained further below, allows Zoom access to unencrypted video and audio from meetings.

36. The following screenshots, which were taken from a March 14, 2020 version of Zoom's official website, show that Zoom claimed to offer end-to-end encryption:

Protecting your Meetings

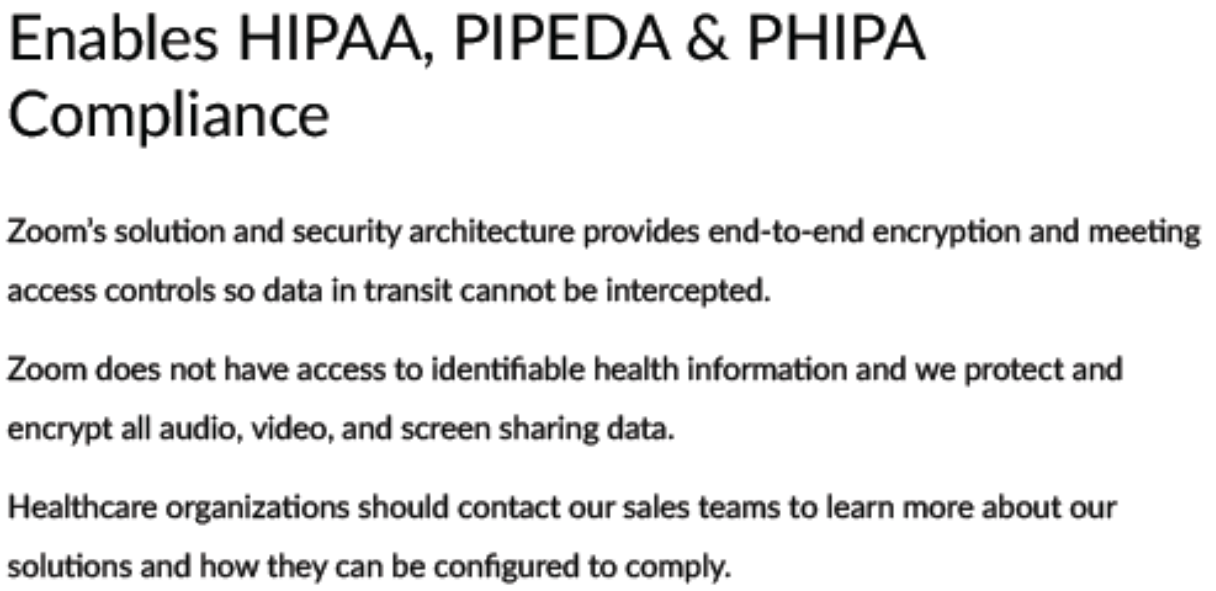
The following in-meeting security capabilities are available to the meeting host:

- Secure a meeting with end-to-end encryption
- Create Waiting Rooms for attendees
- Require host to be present before meeting starts
- Expel a participant or all participants
- Lock a meeting
- Screen share watermarks
- Audio signatures (https://web.archive.org/web/20200314182730/https://www.youtube.com/embed/fYqUoXDqJIw?rel=0&autoplay=1&showinfo=0)
- Enable/disable a participant or all participants to record
- Temporary pause screen-sharing when a new window is opened
- Password protect a meeting
- Only allow individuals with a given e-mail domain to join



Protecting your Data

End-to-End Chat Encryption allows for a secured communication where only the intended recipient can read the secured message. Zoom uses both asymmetric and symmetric algorithms to encrypt the chat session. Session keys are generated with a device-unique hardware ID to avoid data being read from other devices. This ensures that the session can not be eavesdropped on or tampered with.



Enables HIPAA, PIPEDA & PHIPA Compliance

Zoom's solution and security architecture provides end-to-end encryption and meeting access controls so data in transit cannot be intercepted.

Zoom does not have access to identifiable health information and we protect and encrypt all audio, video, and screen sharing data.

Healthcare organizations should contact our sales teams to learn more about our solutions and how they can be configured to comply.

37. In Zoom's white paper, dated June 2019, there was a list of "pre-meeting security capabilities" that are available to the meeting host that starts with "Enable an end-to-end (E2E) encrypted meeting." Later in the white paper, it explained that "E2E Chat Encryption: Zoom E2E chat encryption allows for a secured communication where only the intended recipient can read the secured message. Zoom uses public and private key to encrypt the chat session with Advanced Encryption Standard (AES-256). Session keys are generated with a device-unique hardware ID to avoid data being read from other devices. This ensures that the session can not be eavesdropped on or tampered with."

38. End-to-end encryption is "the most secure" form of privacy for online communications. (ProtonMail, End-to-End Encryption, https://protonmail.com/blog/what-is-end-to-end-encryption/ (last visited, April 3, 2020).) End-to-end encryption security systems encrypt the data transmitted in such a way that that only the participants in the meeting have the ability to decrypt it which prevents anyone monitoring the network from accessing the information users have communicated. In other words, the only users have who have access to shared information are the sender and receiver. This keeps user information and data private and less vulnerable to hacking.

39. A March 31, 2020 article in the Intercept revealed that Zoom does not utilize end-to-end encryption. (Micah Lee & Yael Grauer, Zoom Meetings Aren't End-to-End Encrypted, Despite Misleading Marketing, THE INTERCEPT, https://theintercept.com/2020/03/31/zoom-meeting-encryption/ ("Lee") (last visited, April 3, 2020).) The encryption that Zoom uses to protect meetings is actually transport encryption, or TLS, which is the significantly less secure technology that web servers use to secure HTTPS websites. Transport encryption is different from end-to-end encryption because Zoom itself can access the unencrypted video and audio content of Zoom meetings.

40. Zoom admitted that its video meetings are not actually end-to-end encrypted. In particular, a Zoom spokesperson wrote, "Currently, it is not possible to enable E2E encryption for Zoom video meetings. Zoom video meetings use a combination of TCP and UDP. TCP connections are made using TLS and UDP connections are encrypted with AES using a key negotiated over a TLS connection." (Lee.)

Other Websites Have Access to User Webcams

41. Zoom suffered from a vulnerability that allowed any website to forcibly join a user to a Zoom call, with their video camera activated, without the user's permission. In particular, Motherboard reported on July 9, 2019 that Zoom issued a security patch for Mac users that contained an error that allowed hackers to access user webcams without their knowledge or consent. (Joseph Cox, Zoom Vulnerability Lets Hackers Hijack Your Webcam, MOTHERBOARD, https://www.vice.com/en_us/article/8xzjj4/zoom-video-conferencing-vulnerability-lets-hackers-turn-on-your-webcam (last visited April 3, 2020).) To gain access, a hacker simply needed to embed a short coding sequence into their website which allows the hacker to forcibly join users into a Zoom call with the user's video camera activated.

42. Zoom acknowledged this problem and offered a "solution" which was to provide users the option to have their video setting turned off when they join a new meeting. (https://blog.zoom.us/wordpress/2019/07/08/response-to-video-on-concern/) However, Zoom cannot expect users to uniformly adapt to this setting as the video features are a popular functionality, and millions of webcams are vulnerable to attack.

Zoombombing

43. Zoom also has a vulnerability that allows hackers to "Zoombomb" a Zoom meeting. In particular, "Zoombombing" occurs when a hacker who finds a Zoom link shared on a public channel accesses a meeting that does not require a password, and abuses the chat, screen-sharing and file transfer privileges that the meeting organizer has not restricted. For example, the Boston office of the Federal Bureau of Investigation issued a warning saying that it had received multiple reports from Massachusetts schools about Zoombombers displaying pornography, white supremacist imagery and threatening language during students' calls. The Product does not adequately protect users from the risk of Zombombing and Zoom does not disclose this risk to users.

Hosts Can Record Zoom Meetings Without User Consent and Recordings of Private Zoom Meetings are Available on the Internet

44. Zoom enables users to make recordings of meetings without consent of all participants in violation of Cal. Penal Code § 637.2. In particular, Zoom allows the meeting host or other meeting attendees approved by the administrator to record the meeting to cloud or local storage. Instructions for both local recording and cloud recording are available on Zoom's website. (https://support.zoom.us/hc/en-us/articles/201362473-Local-recording and https://support.zoom.us/hc/en-us/articles/203741855-Cloud-). Zoom does not require all users to affirmatively consent to the recording. Nor does it adequately notify all users that the meeting is being recorded. Cloud recordings are saved to Zoom's cloud server. Further, as explained by a TechRepublic article dated March 24, 2020, even if the recording is saved locally, Zoom temporarily stores it for encoding into MP4 format once the meeting has ended. (Brandon Vigliarolo, "How to Record a Zoom Meeting," March 24, 2020, available at https://www.techrepublic.com/article/how-to-record-a-zoom-meeting/ (last accessed April 13, 2020).)

45. The Washington Post found thousands of recordings of Zoom video calls that were left unprotected and viewable on the open web. (Drew Harwell, "Thousands of Zoom Calls Left Exposed on Open Web," April 3, 2020, Washington Post, available at https://www.msn.com/en-us/money/companies/thousands-of-zoom-video-calls-left-exposed-on-open-web/ar-BB128jQI (last accessed April 13, 2020).) Many of the unprotected calls included discussion of highly sensitive PII, such as private therapy sessions, "telehealth" training calls that included people's names and phone numbers, small-business meetings that discussed private company financial statements, and elementary school classes with student information exposed.

46. These videos appear to have been recorded through Zoom's software and saved onto separate online storage space without a password. Moreover, because Zoom names every video recording in an identical way, a simple online search can reveal a long stream of videos elsewhere that anyone can download and watch. In designing their service, Zoom's engineers bypassed some common security features of other videochat programs, such as requiring people to use a unique file name before saving their own videos.

Zoom Leaks User Private Email Addresses

47. Zoom is leaking personal information of at least thousands of users, including their email address and photos, and giving strangers the ability to attempt to start a video call with them through Zoom. Motherboard reported details of this issue on April 1, 2010. (Joseph Cox, "Zoom is Leaking Peoples' Email Addresses and Photos to Strangers," Motherboard, April 1, 2020, available https://www.vice.com/en_us/article/k7e95m/zoom-leaking-email-addresses-photos (last accessed April 13, 2020).). In particular, Zoom has a "Company Directory" setting, which automatically adds other people to a user's lists of contacts if they signed up with an email address that shares the same domain. This is intended to make it easier to find a specific colleague to call when the domain belongs to an individual company. But when certain users sign up for a Zoom account with personal email addresses, without the consent of users, Zoom has pooled them together with thousands of other people as if they all worked for the same company, exposing their personal information to one another. Zoom has not adequately protected these users' information from disclosure and have failed to disclose the risk of such a disclosure to user.

PLAINTIFF'S EXPERIENCE

48. Plaintiff used the product while working from home during the current stay-at-home order. In particular, on March 17, 2010, Plaintiff signed up for a Basic Plan and activated his account. Plaintiff uses his Apple iPhone to access Zoom. He has downloaded, installed, and accessed the iOS version of the Zoom App. Plaintiff participated in Zoom meetings using the Zoom App on at least March 25, 2020 and April 2, 2020.

49. Plaintiff relied upon the privacy policy and advertising of the Product, including Defendant's claims that it would not share user PII with third parties and that the product is private and secure. The privacy policy and advertising statements were prepared and approved by Defendant and its agents and disseminated statewide and nationwide, as well as designed to encourage consumers to use and/or purchase the Product. Plaintiff was not aware, and did not understand, that Zoom would share information with Facebook, LinkedIn, and, upon information and belief, other third parties—including his city and time zone, the time he accessed the Zoom app, his device type, his mobile carrier, and a unique identifier tied to his device that would allow advertisers to specifically target him. He was not aware, and did not understand, that Zoom would allow third parties like Facebook to access this information and combine it with content and information from other sources to create a unique profile of him for advertising purposes. Plaintiff would not have used the Product, if he had known that the advertising as described herein was false, misleading, and/or deceptive. Plaintiff did not consent to the sharing of his PII with any unauthorized party. He had no knowledge that Zoom had authorized this disclosure of his information and he did not consent to it. Plaintiff would continue using Zoom's products and services if he could be assured that Defendant would take adequate security measures to protect his personal information and secure its services going forward.

50. Plaintiff seeks injunctive relief against Defendant for false and misleading advertising in violation of Business and Professions Code Section 17200, *et seq.,* Business and Professions Code Section 17500, *et seq.*, and Civil Code Section 1750, et seq. Plaintiff also seeks injunctive relief against Defendant for its misuse of private user information in violation of the California Consumer Privacy Act.

51. Defendant made and continues to make these false and misleading statements in its advertising of th Pproduct. Defendant continues to misuse PII. Compliance with remedial statues like those underlying this lawsuit will benefit Plaintiff, the putative classes, consumers, and the general public. Compliance is the primary litigation objective of this lawsuit.

52. Upon information and belief, during the course of its false, misleading, and deceptive advertising campaign, hundreds of millions of people have used and purchased Defendant's Prodict. Plaintiff and the Class have suffered injury in fact and have suffered invasion of their privacy rights as a result of Defendant's false representations and misuse of data and information.

CLASS ALLEGATIONS

53. Plaintiff brings this class action lawsuit on behalf of the following proposed class and subclass of similarly situated persons, pursuant to Rule 23(b)(2) and (b)(3) of the Federal Rules of Civil Procedure, defined as follows:

> The Class: All persons who used the Product in the United States during the time period of four years prior to the filing of the complaint through the present.
>
> The California Sublass: All Class Members who reside in the State of California.

54. This action has been brought and may properly be maintained as a class action against Defendant because there is a well-defined community of interest in the litigation and the proposed class is easily ascertainable.

55. Numerosity: Plaintiff does not know the exact size of the Class, but they estimate it is composed of more than 5000 persons. The persons in the Class are so numerous that the joinder of all such persons is impracticable and the disposition of their claims in a class action rather than in individual actions will benefit the parties and the courts.

56. Common Questions Predominate: This action involves common questions of law and fact to the potential classes because each class member's claim derives from the same deceptive, unlawful and/or unfair statements and omissions. The common questions of law and fact predominate over individual questions, as proof of a common or single set of facts will establish the right of each member of the Class to recover. The questions of law and fact common to the Class including, but are not limited to, the following:

a. Whether the marketing, advertising, and other promotional materials for the Product are deceptive and/or unlawful because of misrepresentations and omissions;

b. Whether Defendant violated Plaintiff's and Class Members' privacy rights;

c. Whether Defendant's marketing, advertising, and other promotional materials for the Product was likely to deceive reasonable consumers;

d. Whether Defendant's representations and omissions are material to reasonable consumers;

e. The amount of profits and revenues earned by Defendant as a result of the misconduct;

f. Whether Class Members are entitled to restitution, injunctive and other equitable relief and, if so, what is the nature (and amount) of such relief; and

g. Whether Class Members are entitled to payment of actual, incidental, consequential, exemplary and/or statutory damages plus interest thereon, and if so, what is the nature of such relief.

57. Typicality: Plaintiff's claims are typical of the claims of other members of the Class because, among other things, all such claims arise out of the same wrongful course of conduct in which the Defendant engaged in violation of law as described herein. Further, the damages of each member of the Class were caused directly by Defendant's wrongful conduct in violation of the law as alleged herein. Plaintiff and the Class Members have suffered injury in fact as a result of Defendant's false representations. Plaintiff and the Class Members each purchased and/or used the Product under the false belief that the it had adequate security measures in place and that Defendant would not misuse their PII. Plaintiff and the Class Members would not have purchased and/or used the Product if they had known it does not have adequate security measures in place and that Defendant misuses personal user PII.

58. Adequacy of Representation: Plaintiff will fairly and adequately protect the interests of all Class Members because it is in their best interests to prosecute the claims alleged herein to obtain full compensation due to them for the unfair and illegal conduct of which they

complain. Plaintiff also has no interests that are in conflict with, or antagonistic to, the interests of class members. Plaintiff has retained highly competent and experienced class action attorneys to represent his interests and that of the classes. By prevailing on his own claims, Plaintiff will establish Defendant's liability to all class members. Plaintiff and his counsel have the necessary financial resources to adequately and vigorously litigate this class action, and Plaintiff and counsel are aware of their fiduciary responsibilities to the Class Members and are determined to diligently discharge those duties by vigorously seeking the maximum possible recovery for class members.

59. Superiority: There is no plain, speedy, or adequate remedy other than by maintenance of this class action. The prosecution of individual remedies by members of the classes will tend to establish inconsistent standards of conduct for Defendant and result in the impairment of class members' rights and the disposition of their interests through actions to which they were not parties. Class action treatment will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of effort and expense that numerous individual actions would engender. Furthermore, as the damages suffered by each individual member of the class may be relatively small, the expenses and burden of individual litigation would make it difficult or impossible for individual members of the class to redress the wrongs done to them, while an important public interest will be served by addressing the matter as a class action.

60. Plaintiff is unaware of any difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

CAUSES OF ACTION

PLAINTIFF'S FIRST CAUSE OF ACTION

(Violation of the Consumers Legal Remedies Act (the "CLRA"), California Civil Code § 1750, *et seq., on behalf of the California Subclass*)

61. Plaintiff realleges and incorporates the paragraphs of this Class Action Complaint as if set forth herein.

62. Defendant's actions, representations and conduct have violated, and continue to

violate the CLRA, because they extend to transactions that are intended to result, or which have resulted, in the sale or lease of goods or services to consumers.

63. Plaintiff and other Class Members are "consumers" as that term is defined by the CLRA in California Civil Code § 1761(d).

64. The Products that Plaintiff (and other similarly situated Class Members) purchased or used from Defendant were "goods" within the meaning of California Civil Code § 1761(a).

65. The practices described herein, specifically Defendant's acts and practices described herein were intended to result in the sale and use of the Product to and by the consuming public and have violated, and continue to violate, § 1770(a)(2), § 1770(a)(5), § 1770(a)(7), § 1770(a)(8), and § 1770(a)(9) of the CLRA. In violation of California Civil Code §1770(a)(2), Defendant's acts and practices constitute improper representations regarding the source, sponsorship, approval, or certification of the goods they sold. In violation of California Civil Code §1770(a)(5), Defendant's acts and practices constitute improper representations that the goods they sell have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities, which they do not have, e.g., that the Product is equipped with end-to-end encryption and adequately protects user information with secure privacy measures. In violation of California Civil Code §1770(a)(7), Defendant's acts and practices constitute improper representations that the goods it sells are of a particular standard, quality, or grade, when they are of another. In violation of California Civil Code §1770(a)(8), Defendant has disparaged the goods, services, or business of another by false or misleading representation of fact, e.g., by representing that unlike other video conferencing platforms, it sells and distributes a Product that includes end-to-end encryption. Finally, in violation of California Civil Code §1770(a)(9), Defendant has advertised goods or services with intent not to sell them as advertised.

66. Plaintiff requests that this Court enjoin Defendant from continuing to employ the unlawful methods, acts and practices alleged herein pursuant to California Civil Code § 1780(a)(2). If Defendant is not restrained from engaging in these types of practices in the future, Plaintiff and the other members of the Class will continue to suffer harm.

67. **CIVIL CODE § 1782 NOTICE.** Plaintiff notices and demands that within thirty

(30) days from that date of the filing of this Complaint that Defendant correct, repair, replace or otherwise rectify the unlawful, unfair, false and or deceptive practices complained of herein.

68. Should the violations herein alleged not be corrected, repaired, replace or rectified as required by Civil Code § 1782 within 30 days with respect to all Class Members, Plaintiff will seek to amend this Class Action Complaint to seek, on behalf of each Class Member, actual damages of at least $1000, punitive damages, an award of $5000 for each Class Member who is a disabled person or senior citizen, and restitution of any ill-gotten gains due to Defendant's acts and practices.

69. Plaintiff also requests that this Court award him costs and reasonable attorneys' fees pursuant to California Civil Code § 1780(d).

PLAINTIFF'S SECOND CAUSE OF ACTION

(False Advertising, Business and Professions Code § 17500, *et seq.* ("FAL"), *on behalf of the California Subclass*)

70. Plaintiff realleges and incorporates by reference the paragraphs of this Class Action Complaint as if set forth herein.

71. Beginning at an exact date unknown to Plaintiff, but within three (3) years preceding the filing of the Class Action Complaint, Defendant made untrue, false, deceptive and/or misleading statements in connection with the advertising and marketing of the Product.

72. Defendant made representations and statements (by omission and commission) that led reasonable customers to believe that the Product had adequate security measures in place and that Defendant would not misuse their personal information. Defendant knowingly disseminated misleading claims that the Product is equipped with end-to-end encryption and adequately protects user information with secure privacy measures as a means to mislead the public for financial gain.

73. Plaintiff and those similarly situated relied to their detriment on Defendant's false, misleading and deceptive advertising and marketing practices, including each of the misrepresentations and omissions set forth above. Had Plaintiff and those similarly situated been adequately informed and not intentionally deceived by Defendant, he would have acted differently by, without limitation, refraining from using or purchasing the Product.

74. Defendant's acts and omissions are likely to deceive the general public.

75. Defendant engaged in these false, misleading and deceptive advertising and marketing practices to increase its profits. Accordingly, Defendant has engaged in false advertising, as defined and prohibited by section 17500, *et seq.* of the California Business and Professions Code.

76. The aforementioned practices, which Defendant used, and continues to use, to its significant financial gain, also constitutes unlawful competition and provides an unlawful advantage over Defendant's competitors as well as injury to the general public.

77. As a direct and proximate result of such actions, Plaintiff and the other similarly situated Class Members have suffered, and continue to suffer, injury in fact and have lost money and/or property as a result of such false, deceptive and misleading advertising in an amount which will be proven at trial, but which is in excess of the jurisdictional minimum of this Court.

78. Plaintiff seeks, on behalf of himself and those similarly situated, full restitution of monies, as necessary and according to proof, to restore any and all monies acquired by Defendant from Plaintiff, the general public, or those similarly situated by means of the false, misleading and deceptive advertising and marketing practices complained of herein, plus interest thereon.

79. Plaintiff seeks, on behalf of himself and those similarly situated, a declaration that the above-described practices constitute false, misleading and deceptive advertising.

80. Plaintiff seeks, on behalf of himself and those similarly situated, an injunction to prohibit Defendant from continuing to engage in the false, misleading and deceptive advertising and marketing practices complained of herein. Such misconduct by Defendant, unless and until enjoined and restrained by order of this Court, will continue to cause injury in fact to the general public and the loss of money and property in that Defendant will continue to violate the laws of California, unless specifically ordered to comply with the same. This expectation of future violations will require current and future consumers to repeatedly and continuously seek legal redress in order to recover monies paid to Defendant to which it is not entitled. Plaintiff, those similarly situated and/or other consumers nationwide have no other adequate remedy at law to ensure future compliance with the California Business and Professions Code alleged to have been

violated herein.

PLAINTIFF'S THIRD CAUSE OF ACTION
(Common Law Fraud, Deceit and/or Misrepresentation, *on behalf of the Class*)

81. Plaintiff realleges and incorporates by reference the paragraphs of this Class Action Complaint as if set forth herein.

82. Defendant has fraudulently and deceptively informed Plaintiff that the Product had adequate security measures in place and that Defendant would not misuse their personal information. Further, Defendant failed to disclose the Product's known security risks and that Defendant disclosed users' private information to third parties.

83. These misrepresentations and omissions were known exclusively to, and actively concealed by, Defendant, not reasonably known to Plaintiff, and material at the time they were made. Defendant knew that the Product has known security risks and that Defendant disclosed users' personal information to third parties. Defendant's misrepresentations and omissions concerned material facts that were essential to the analysis undertaken by Plaintiff as to whether to use and/or purchase the Product. In misleading Plaintiff and not so informing Plaintiff, Defendant breached its duty to him. Defendant also gained financially from, and as a result of, its breach.

84. Plaintiff and those similarly situated relied to their detriment on Defendant's misrepresentations and fraudulent omissions. Had Plaintiff and those similarly situated been adequately informed and not intentionally deceived by Defendant, they would have acted differently by, without limitation: (i) declining to purchase or use the Product, (ii) purchasing or using the Product less, or (iii) paying less for the Product.

85. By and through such fraud, deceit, misrepresentations and/or omissions, Defendant intended to induce Plaintiff and those similarly situated to alter their position to their detriment. Specifically, Defendant fraudulently and deceptively induced Plaintiff and those similarly situated to, without limitation, purchase and use the Product.

86. Plaintiff and those similarly situated justifiably and reasonably relied on Defendant's misrepresentations and omissions, and, accordingly, were damaged by Defendant.

87. As a direct and proximate result of Defendant's misrepresentations and/or

omissions, Plaintiff and those similarly situated have suffered damages, including, without limitation, the amount they paid for the Product and the value of their personal information shared with third parties.

88. Defendant's conduct as described herein was wilful and malicious and was designed to maximize Defendant's profits even though Defendant knew that it would cause loss and harm to Plaintiff and those similarly situated.

PLAINTIFF'S FOURTH CAUSE OF ACTION
(Unlawful, unfair, and fraudulent trade practices violation of Business and Professions Code § 17200, *et seq., on behalf of the California Subclass*)

89. Plaintiff realleges and incorporates by reference the paragraphs of this Class Action Complaint as if set forth herein.

90. Within four (4) years preceding the filing of this lawsuit, and at all times mentioned herein, Defendant has engaged, and continues to engage, in unlawful, unfair, and fraudulent trade practices in California by engaging in the unlawful, unfair, and fraudulent business practices outlined in this complaint.

91. In particular, Defendant has engaged, and continues to engage, in unlawful practices by, without limitation, violating the following state and federal laws: (i) the CLRA as described herein; (ii) the FAL as described herein; (iii) the CCPA as described herein; and (iv) Cal. Penal Code § 637.2 as described herein.

92. In particular, Defendant has engaged, and continues to engage, in unfair and fraudulent practices by, without limitation, the following: (i) misrepresenting that the Product has adequate security measures in place; (ii) misrepresenting that Defendant would not misuse their personal information; (iii) failing to disclose known security risks associated with using the Product; and (iv) failing to disclose Defendant's disclosure of users' personal information to third parties.

93. Plaintiff and those similarly situated relied to their detriment on Defendant's unlawful, unfair, and fraudulent business practices. Had Plaintiff and those similarly situated been adequately informed and not deceived by Defendant, they would have acted differently by, declining to purchase or use the Product.

94. Defendant's acts and omissions are likely to deceive the general public.

95. Defendant engaged in these deceptive and unlawful practices to increase its profits. Accordingly, Defendant has engaged in unlawful trade practices, as defined and prohibited by section 17200, *et seq.* of the California Business and Professions Code.

96. The aforementioned practices, which Defendant has used to its significant financial gain, also constitute unlawful competition and provide an unlawful advantage over Defendant's competitors as well as injury to the general public.

97. As a direct and proximate result of such actions, Plaintiff and the other class members, have suffered and continue to suffer injury in fact and have lost money and/or property as a result of such deceptive and/or unlawful trade practices and unfair competition in an amount which will be proven at trial, but which is in excess of the jurisdictional minimum of this Court. Among other things, Plaintiff and the Class Members lost the amount they paid for the Product and/or the value of the PII that was wrongfully taken from them.

98. As a direct and proximate result of such actions, Defendant has enjoyed, and continues to enjoy, significant financial gain in an amount which will be proven at trial, but which is in excess of the jurisdictional minimum of this Court.

99. Plaintiff seeks, on behalf of themselves and those similarly situated, full restitution of monies, as necessary and according to proof, to restore any and all monies acquired by Defendant from Plaintiff, the general public, or those similarly situated by means of the deceptive and/or unlawful trade practices complained of herein, plus interest thereon.

100. Plaintiff seeks, on behalf of those similarly situated, a declaration that the above-described trade practices are fraudulent, unfair, and/or unlawful.

101. Plaintiff seeks, on behalf of those similarly situated, an injunction to prohibit Defendant from continuing to engage in the deceptive and/or unlawful trade practices complained of herein. Such misconduct by Defendant, unless and until enjoined and restrained by order of this Court, will continue to cause injury in fact to the general public and the loss of money and property in that Defendant will continue to violate the laws of California, unless specifically ordered to comply with the same. This expectation of future violations will require current and

future consumers to repeatedly and continuously seek legal redress in order to recover monies paid to Defendant to which they were not entitled. Plaintiff, those similarly situated and/or other consumers nationwide have no other adequate remedy at law to ensure future compliance with the California Business and Professions Code alleged to have been violated herein.

PLAINTIFF'S FIFTH CAUSE OF ACTION
(Violation of the California Consumer Privacy Act
Cal. Civ. Code § 1789.100, et seq., *on behalf of the California Subclass*)

102. Plaintiff realleges and incorporates by reference all paragraphs alleged herein

103. Defendant has violated California Civil Code Section 1798.100(b) of the California Consumer Privacy Act ("CCPA") by collecting and sharing private user information without providing adequate notice.

104. Defendant collects personal user information as defined in Civil Code Section 1789.140, such as their location.

105. Defendant has violated California Civil Code Section 1798.150(a). As a result of Defendant's inability to implement and maintain reasonable security procedures and practices, Defendant has given Facebook, LinkedIn, and other third parties unauthorized access to private user information as alleged herein.

106. Defendant has violated its duty to protect the personal information of Plaintiff and the Class.

107. Defendant's violation of its duty directly and proximately caused Plaintiff and members of the Class to have their personal information collected and shared with Facebook, LinkedIn, and other third parties without authorization. Upon information and belief, Defendant is sharing user information with other unknown parties in the same manner as alleged herein.

108. Plaintiff and the California Subclass were injured through violations of legally protected privacy interests, in the form of unauthorized disclosure of personal user information.

109. Defendant knew or should have known that it was violating the CCPA by sharing unauthorized information with Facebook. Defendant also failed to safeguard private user information and maintain reasonable security procedures.

110. Defendant is a corporation that is organized and operated for the financial benefit

of its owners.

111. On behalf of the California Subclass, Plaintiff seeks an order enjoining Defendant from continuing to violate the CCPA as alleged herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and those similarly situated, respectfully requests that the Court enter judgment against Defendant as follows:

A. Certification of the proposed Class and Subclasses, including appointment of Plaintiff's counsel as class counsel;

B. An order temporarily and permanently enjoining Defendant from continuing the unlawful, deceptive, fraudulent, and unfair business practices alleged in this Complaint;

C. As to causes of action 2 & 3, an award of compensatory damages in an amount to be determined at trial;

D. An award of statutory damages in an amount to be determined at trial;

E. As to causes of action 2 & 3, an award of punitive damages in an amount to be determined at trial;

F. As to causes of action 2, 3 & 4, an award of restitution in an amount to be determined at trial;

G. An order requiring Defendant to pay both pre- and post-judgment interest on any amounts awarded;

H. For reasonable attorney's fees and the costs of suit incurred; and

I. For such further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury.

Dated: April 14, 2020

GUTRIDE SAFIER LLP

/s Seth A. Safier

Adam J. Gutride, Esq.
Seth A. Safier, Esq.
Marie McCrary, Esq.
100 Pine Street, Suite 1250
San Francisco, CA 94111

Exhibit A

EXHIBIT A

I, Robert Lawton, declare:

1. I am the Plaintiff in this action. If called upon to testify, I could and would competently testify to the matters contained herein based upon my personal knowledge.

2. I submit this Declaration pursuant to California Code of Civil Procedure section 2215.5 and California Civil Code section 1780(d).

3. I downloaded and used the Zoom application at issue in this case in March 2020 while in San Francisco, California.

I declare under penalty of perjury under the laws of California that the foregoing is true and correct.

Executed this 14th day of April 2020, in San Francisco, California.

DocuSigned by:
Robert Lawton
1171BEF16DDC4F2...
Robert Lawton