

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

6 Attorneys for Plaintiff

7 UNITED STATES DISTRICT COURT FOR THE
8 NORTHERN DISTRICT OF CALIFORNIA
9

10 ROBERT LAWTON, as an individual, on behalf
11 of himself, the general public and those similarly
12 situated,

13 Plaintiff,

14 v.

15 ZOOM VIDEO COMMUNICATIONS, INC.,

16 Defendant.
17
18
19
20
21
22
23
24
25
26
27
28

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

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

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

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

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

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

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

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

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

7 **PARTIES**

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

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

17 **JURISDICTION AND VENUE**

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

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

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

1 continuous business practices in the State of California.

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

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

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

9 **SUBSTANTIVE ALLEGATIONS**

10 17. Defendant provides an online platform for video and audio conferencing, collabo-
11 ration, chat, and webinars. Defendant promises customers that its products allow them to “meet
12 securely” though “end-to-end encryption for all meetings, role-based user security, password pro-
13 tection, waiting rooms, and place attendee on hold.” Zoom’s chief product is “Zoom Meetings”
14 (the “Product”). Zoom has emerged as a fundamental online utility, with 200 million daily users
15 — including family members gathering to celebrate holidays, teachers leading online classes for
16 students and members of Alcoholics Anonymous holding meetings. (Zoom Blog, A Message to
17 Our Users, <https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/> (last visited April
18 3, 2020).)

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

24 19. Zoom has profited off of users’ desire to stay connected professionally and per-
25 sonally during the global pandemic and the accompanying stay-at-home orders. Zoom’s stock
26 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

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

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

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

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

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

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

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

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

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

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

24 31. Moreover, the ostensibly corrected Zoom App does nothing to remedy the unau-
25 thorized disclosures made by Zoom to date. Zoom has not ensured that Facebook (or anyone else,
26 including others with whom Facebook has shared this personal information) has deleted all the
27 PII that it received from Zoom without adequate notice or authorization by Zoom's users. Finally,
28

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

3 **Zoom Shares Private LinkedIn Information With Users**

4 32. A data-mining feature on the Product allowed participants to access LinkedIn pro-
5 file data about other users who signed into the meeting— without asking for their permission dur-
6 ing the meeting or even notifying them that their LinkedIn data was available to other users.

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

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

25 **Zoom Falsely Advertises that its Software is Secure**

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

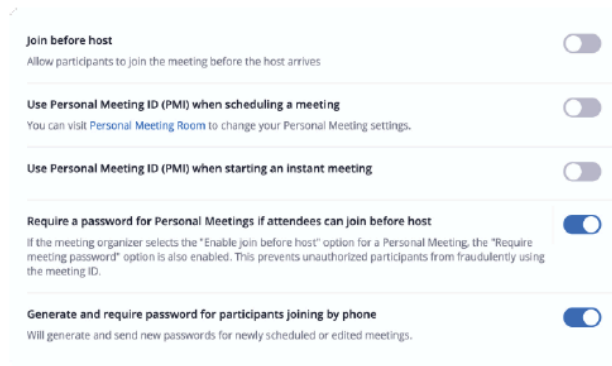
Zoom’s advertising statements to determine which product to use and purchase. However, this is false, deceptive, and misleading because Zoom does not use end-to-end encryption and instead it offers what is usually called transport encryption, which, as explained further below, allows Zoom access to unencrypted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

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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.

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

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

14 **Other Websites Have Access to User Webcams**

15 41. Zoom suffered from a vulnerability that allowed any website to forcibly join a user
16 to a Zoom call, with their video camera activated, without the user’s permission. In particular,
17 Motherboard reported on July 9, 2019 that Zoom issued a security patch for Mac users that con-
18 tained an error that allowed hackers to access user webcams without their knowledge or consent.
19 (Joseph Cox, Zoom Vulnerability Lets Hackers Hijack Your Webcam, MOTHERBOARD,
20 [https://www.vice.com/en_us/article/8xzjj4/zoom-video-conferencing-vulnerability-lets-hackers-
21 turn-on-your-webcam](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 em-
22 bed a short coding sequence into their website which allows the hacker to forcibly join users into
23 a Zoom call with the user’s video camera activated.

24 42. Zoom acknowledged this problem and offered a “solution” which was to provide
25 users the option to have their video setting turned off when they join a new meeting.
26 (<https://blog.zoom.us/wordpress/2019/07/08/response-to-video-on-concern/>) However, Zoom
27 cannot expect users to uniformly adapt to this setting as the video features are a popular function-
28 ality, 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).)

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

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

15 **Zoom Leaks User Private Email Addresses**

16 47. Zoom is leaking personal information of at least thousands of users, including their
17 email address and photos, and giving strangers the ability to attempt to start a video call with
18 them through Zoom. Motherboard reported details of this issue on April 1, 2010. (Joseph Cox,
19 “Zoom is Leaking Peoples’ Email Addresses and Photos to Strangers,” Motherboard, April 1,
20 2020, available [https://www.vice.com/en_us/article/k7e95m/zoom-leaking-email-addresses-](https://www.vice.com/en_us/article/k7e95m/zoom-leaking-email-addresses-photos)
21 [photos](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,
22 which automatically adds other people to a user’s lists of contacts if they signed up with an email
23 address that shares the same domain. This is intended to make it easier to find a specific colleague
24 to call when the domain belongs to an individual company. But when certain users sign up for a
25 Zoom account with personal email addresses, without the consent of users, Zoom has pooled
26 them together with thousands of other people as if they all worked for the same company, expos-
27 ing their personal information to one another. Zoom has not adequately protected these users’ in-
28 formation from disclosure and have failed to disclose the risk of such a disclosure to user.

PLAINTIFF'S EXPERIENCE

1
2 48. Plaintiff used the product while working from home during the current stay-at-
3 home order. In particular, on March 17, 2010, Plaintiff signed up for a Basic Plan and activated
4 his account. Plaintiff uses his Apple iPhone to access Zoom. He has downloaded, installed, and
5 accessed the iOS version of the Zoom App. Plaintiff participated in Zoom meetings using the
6 Zoom App on at least March 25, 2020 and April 2, 2020.

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

24 50. Plaintiff seeks injunctive relief against Defendant for false and misleading adver-
25 tising in violation of Business and Professions Code Section 17200, *et seq.*, Business and Profes-
26 sions Code Section 17500, *et seq.*, and Civil Code Section 1750, *et seq.* Plaintiff also seeks
27 injunctive relief against Defendant for its misuse of private user information in violation of the
28 California Consumer Privacy Act.

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

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

9 **CLASS ALLEGATIONS**

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

13 The Class: All persons who used the Product in the United States during the time period
14 of four years prior to the filing of the complaint through the present.

15 The California Subclass: All Class Members who reside in the State of California.

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

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

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

- 1 a. Whether the marketing, advertising, and other promotional materials for the
- 2 Product are deceptive and/or unlawful because of misrepresentations and
- 3 omissions;
- 4 b. Whether Defendant violated Plaintiff's and Class Members' privacy rights;
- 5 c. Whether Defendant's marketing, advertising, and other promotional materials for
- 6 the Product was likely to deceive reasonable consumers;
- 7 d. Whether Defendant's representations and omissions are material to reasonable
- 8 consumers;
- 9 e. The amount of profits and revenues earned by Defendant as a result of the
- 10 misconduct;
- 11 f. Whether Class Members are entitled to restitution, injunctive and other equitable
- 12 relief and, if so, what is the nature (and amount) of such relief; and
- 13 g. Whether Class Members are entitled to payment of actual, incidental,
- 14 consequential, exemplary and/or statutory damages plus interest thereon, and if so,
- 15 what is the nature of such relief.

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

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

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

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

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

22 CAUSES OF ACTION

23 PLAINTIFF'S FIRST CAUSE OF ACTION

24 **(Violation of the Consumers Legal Remedies Act (the "CLRA"), California Civil Code §**
25 **1750, et seq., on behalf of the California Subclass)**

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

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

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

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

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

7 65. The practices described herein, specifically Defendant’s acts and practices
8 described herein were intended to result in the sale and use of the Product to and by the
9 consuming public and have violated, and continue to violate, § 1770(a)(2), § 1770(a)(5),
10 § 1770(a)(7), § 1770(a)(8), and § 1770(a)(9) of the CLRA. In violation of California Civil Code
11 §1770(a)(2), Defendant’s acts and practices constitute improper representations regarding the
12 source, sponsorship, approval, or certification of the goods they sold. In violation of California
13 Civil Code §1770(a)(5), Defendant’s acts and practices constitute improper representations that
14 the goods they sell have sponsorship, approval, characteristics, ingredients, uses, benefits, or
15 quantities, which they do not have, e.g., that the Product is equipped with end-to-end encryption
16 and adequately protects user information with secure privacy measures. In violation of California
17 Civil Code §1770(a)(7), Defendant’s acts and practices constitute improper representations that
18 the goods it sells are of a particular standard, quality, or grade, when they are of another. In
19 violation of California Civil Code §1770(a)(8), Defendant has disparaged the goods, services, or
20 business of another by false or misleading representation of fact, e.g., by representing that unlike
21 other video conferencing platforms, it sells and distributes a Product that includes end-to-end
22 encryption. Finally, in violation of California Civil Code §1770(a)(9), Defendant has advertised
23 goods or services with intent not to sell them as advertised.

24 66. Plaintiff requests that this Court enjoin Defendant from continuing to employ the
25 unlawful methods, acts and practices alleged herein pursuant to California Civil Code
26 § 1780(a)(2). If Defendant is not restrained from engaging in these types of practices in the
27 future, Plaintiff and the other members of the Class will continue to suffer harm.

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

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

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

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

11 **PLAINTIFF'S SECOND CAUSE OF ACTION**
12 **(False Advertising, Business and Professions Code § 17500, *et seq.* ("FAL"), *on behalf of the***
13 ***California Subclass*)**

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

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

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

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

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

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

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

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

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

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

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

1 violated herein.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

12 104. Defendant collects personal user information as defined in Civil Code Section
13 1789.140, such as their location.

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

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

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

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

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

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

1 of its owners.

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

4 **PRAYER FOR RELIEF**

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

- 7 A. Certification of the proposed Class and Subclasses, including appointment of Plain-
8 tiff's counsel as class counsel;
- 9 B. An order temporarily and permanently enjoining Defendant from continuing the un-
10 lawful, deceptive, fraudulent, and unfair business practices alleged in this Complaint;
- 11 C. As to causes of action 2 & 3, an award of compensatory damages in an amount to be
12 determined at trial;
- 13 D. An award of statutory damages in an amount to be determined at trial;
- 14 E. As to causes of action 2 & 3, an award of punitive damages in an amount to be deter-
15 mined at trial;
- 16 F. As to causes of action 2, 3 & 4, an award of restitution in an amount to be determined
17 at trial;
- 18 G. An order requiring Defendant to pay both pre- and post-judgment interest on any
19 amounts awarded;
- 20 H. For reasonable attorney's fees and the costs of suit incurred; and
- 21 I. For such further relief as this Court may deem just and proper.

22 **JURY TRIAL DEMANDED**

23 Plaintiff hereby demands a trial by jury.

24 Dated: April 14, 2020

GUTRIDE SAFIER LLP

25 /s/ Seth A. Safier
26 Adam J. Gutride, Esq.
27 Seth A. Safier, Esq.
28 Marie McCrary, Esq.
100 Pine Street, Suite 1250
San Francisco, CA 94111

Exhibit A

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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

CIVIL COVER SHEET

The JS-CAND 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

I. (a) PLAINTIFFS

ROBERT LAWTON

San Francisco

(b) County of Residence of First Listed Plaintiff (EXCEPT IN U.S. PLAINTIFF CASES)

Seth Safer, Gutridge Safer LLP, 100 Pine St., #1250, SF, CA 94111, 415-366-6545; seth@gutridesafer.com

DEFENDANTS

ZOOM VIDEO COMMUNICATIONS, INC.

County of Residence of First Listed Defendant (IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- 1 U.S. Government Plaintiff
2 U.S. Government Defendant
3 Federal Question (U.S. Government Not a Party)
4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

Table with columns for Plaintiff (PTF) and Defendant (DEF) citizenship: Citizen of This State, Citizen of Another State, Citizen or Subject of a Foreign Country, Incorporated or Principal Place of Business In This State, Incorporated and Principal Place of Business In Another State, Foreign Nation.

IV. NATURE OF SUIT (Place an "X" in One Box Only)

Large table with categories: CONTRACT, REAL PROPERTY, TORTS, CIVIL RIGHTS, PRISONER PETITIONS, HABEAS CORPUS, OTHER, FORFEITURE/PENALTY, LABOR, IMMIGRATION, BANKRUPTCY, SOCIAL SECURITY, FEDERAL TAX SUITS, OTHER STATUTES.

V. ORIGIN (Place an "X" in One Box Only)

- 1 Original Proceeding
2 Removed from State Court
3 Remanded from Appellate Court
4 Reinstated or Reopened
5 Transferred from Another District (specify)
6 Multidistrict Litigation-Transfer
8 Multidistrict Litigation-Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity): 28 USC S. 1332

Brief description of cause: class action complaint for violation of consumer protection statutes; fraud; privacy violation

VII. REQUESTED IN COMPLAINT:

CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, Fed. R. Civ. P. DEMAND \$ JURY DEMAND: Yes No

VIII. RELATED CASE(S), IF ANY (See instructions):

JUDGE Lucy Koh DOCKET NUMBER 5:20-cv-02155-LHK

IX. DIVISIONAL ASSIGNMENT (Civil Local Rule 3-2)

(Place an "X" in One Box Only) SAN FRANCISCO/OAKLAND SAN JOSE EUREKA-MCKINLEYVILLE

DATE April 14, 2020

SIGNATURE OF ATTORNEY OF RECORD

s/Seth A. Safer/s/