BOTTINI & BOTTINI, INC.
Francis A. Bottini, Jr. (SBN 175783)
fbottini@bottinilaw.com
Albert Y. Chang (SBN 296065)
achang@bottinilaw.com
Yury A. Kolesnikov (SBN 271173)
ykolesnikov@bottinilaw.com
7817 Ivanhoe Avenue, Suite 102
La Jolla, California 92037
Telephone: (858) 914-2001
Facsimile: (858) 914-2002

COTCHETT, PITRE & MCCARTHY, LLP
Mark C. Molumphy (SBN 168009)
mmolumphy@cpmlegal.com
Tyson Redenbarger (SBN 294424)
tredenbarger@cpmlegal.com
Anya N. Thepot (SBN 318430)
athepot@cpmlegal.com
San Francisco Airport Office Center
840 Malcolm Road, Suite 200
Burlingame, California 94010
Telephone: (650) 697-6000
Facsimile: (650) 697-0577

Attorneys for Plaintiffs and the Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

SAINT PAULUS LUTHERAN CHURCH and HEDDI N. CUNDLE, individually and on behalf of themselves and all others similarly situated, Plaintiffs, vs. ZOOM VIDEO COMMUNICATIONS, INC., Defendant.	Case No. _____ Class Action **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

1. Plaintiffs Saint Paulus Lutheran Church ("Saint Paulus") and Heddi N. Cundle (together, "Plaintiffs"), on behalf of themselves and all others similarly situated (the "Class," as defined in paragraph 94 below), submit this complaint against defendant Zoom Video Communications, Inc. ("Zoom") for, among other things, negligence, breach of implied contract, and violations of the California Consumer Privacy Act ("CCPA"), the Consumers Legal Remedies Act ("CLRA"), and the Unfair Competition Law ("UCL"). In support of these claims, Plaintiffs allege the following (a) upon personal knowledge with respect to the matters pertaining to themselves; and (b) upon information and belief with respect to all other matters, based upon, among other things, the investigations undertaken by Plaintiffs' counsel. Plaintiffs believe that substantial additional evidentiary support will exist for the allegations set forth below after a reasonable opportunity for discovery.

INTRODUCTION

2. Saint Paulus, one of the oldest churches in San Francisco, is a sanctuary for San Franciscans of all walks of life to pray and worship. Known to be "an inclusive community of God's diverse people visible in the world," Saint Paulus welcomes all people — in the words of its longtime pastor, the Reverend Daniel Solberg, "all God's children" — and focuses on caring for the marginalized and the underserved. At this turbulent time of a pandemic, the importance of the sanctity of Saint Paulus cannot be overstated.

3. But Zoom — a multibillion-dollar tech giant experiencing exponential growth as a result of the COVID-19 pandemic — violated this sanctity. Instead of providing Saint Paulus and its congregants with a password-protected and secure videoconferencing platform, Zoom allowed a "known offender" — one who "has been reported multiple times to the authorities" — to Zoombomb Saint Paulus's May 6, 2020 bible-study class. As a result, Ms. Cundle, Saint Paulus's administrator, and other attendees of the bible-study class — most of whom were senior citizens — had their computer screens hijacked and their control buttons disabled while being forced to watch pornographic video footages. The footages were sick and sickening — portraying adults engaging in sexual acts with each other and

performing sexual acts on infants and children, in addition to physically abusing them.

4. Because of Zoom's utter failure in providing security, Saint Paulus's bible-study class was Zoombombed twice within minutes. Traumatized and helpless, Ms. Cundle and Saint Paulus's congregants ended their bible-study class. Immediately Ms. Cundle immediately reached out to Zoom and demanded action to rectify the situation and to improve security for future videoconferences. But Zoom did nothing.

5. Unfortunately, Saint Paulus, its congregants, and Ms. Cundle were not the only victims of Zoombombing. Indeed, many other Zoom users,[1] including schoolchildren,[2] fell victim to similar deeply disturbing and traumatizing experiences due to Zoom's failure to maintain adequate security in Zoom videoconferences.[3] As detailed below, Zoom prioritizes profit and revenue over data protection and user security while millions of users in the United States registered with Zoom based on its false advertisements and rely on Zoom's platform to conduct their business during this pandemic.

6. On behalf of Plaintiffs and other similarly situated Class members, this class action seeks equitable relief against Zoom and damages sustained by the Class as a result of Zoom's:

- unlawful sharing of users' personal information with third parties, including Facebook, Inc., without adequate notice to or authorization from users;
- failure to safeguard its users' confidential, sensitive personal information;

---

[1] Coleen Shalby, *"Disturbing Zoom-Bombing" Incident Hits Fresno State Students, Officials Say*, L.A. TIMES, Apr. 23, 2020, *available at* https://www.latimes.com/ California /story/2020-04-23/coronaviruszoom-bombing-fresno-state (last visited May 11, 2020).

[2] Valarie Honeycutt Spears, *Pornographic Video Appeared During "Zoom Bombing" in a KY School Virtual Meeting*, LEXINGTON HERALD LEADER, Apr. 7, 2020, *available at* https://www.kentucky.com/news/local/education/article241809326.html (last visited May 11, 2020).

[3] *FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic*, FBI (Mar. 30, 2020), *available at* https://www.fbi.gov/contact-us/field offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-class room-hijackingduring-covid-19-pandemic (last visited May 11, 2020).

- failure to provide adequate security, as promised, to avoid breach and infiltration (*e.g.*, "Zoombombing") of users' videoconferences; and
- unfair, unlawful, and deceptive business practices relating to Zoom's data security.

7. Zoom provides video-communication services using a cloud platform for video and audio conferencing, collaboration, chat, and webinars. Founded in 2011, Zoom became a publicly traded company just a year ago (in April 2019), and reported over $622,658,000 in revenue for the fiscal year ending January 31, 2020. Today, Zoom has a market capitalization exceeding $30 billion. Millions of consumers use Zoom's services daily.

8. In the wake of the global COVID-19 pandemic, demand for Zoom's services exploded because hundreds of millions of people — all under stay-at-home orders — resort to videoconferencing to connect with others for work and social functions. In recent weeks, Zoom has become the virtual classroom for millions of schoolchildren and workspace for many businesses and government agencies. The number of meeting participants across Zoom has jumped from 10 million in December 2019 to 200 million in March 2020.

9. As the usage of Zoom's services skyrockets, so do its collection and use of users' personal information. And the importance of security of Zoom's videoconferences cannot be overstated because Zoom provides services to many critical government agencies responsible for combating the COVID-19 pandemic, including the Center for Disease Control and Prevention ("CDC") and the U.S. Department of Homeland Security ("DHS").[4]

10. While Zoom enjoyed its success due to the hike of revenues and its stock price resulting from the explosion of demands for its services, Zoom's unlawful collection and use of users' personal information and its lack of adequate security came to light in a series of

[4] Zoom for Government, *available at* https://zoom.us/government (last visited Apr. 6, 2020) (featuring photos of law enforcement and military personnel at work and listing under "Organizations that love Zoom" eight government agencies, including the CDC, DHS, the Colorado Department of Corrections, the Hawaii State Department of Health, the Los Angeles Police Department, and the City of San Jose).

articles published in late March and early April 2020 in *Vice*,[5] *The New York Times*,[6] the *Washington Post*,[7] *The Wall Street Journal*,[8] and other news outlets.[9]

11. As revealed in these news reports, Zoom uses data-mining tools to collect users' personal information and shares it with third parties without users' consent. Zoom allows these third parties to use such personal information to target users with advertisements.

12. Zoom also fails to implement proper security measures to protect users' privacy and secure their videoconferences. As a result, "Zoombombing" by uninvited participants has become frequent. Contrary to Zoom's promises, Zoom's videoconferences are not end-to-end (also known as "E2E") encrypted — which means that in addition to the participating users, Zoom has the technical ability to spy on the videoconferences and, when compelled by the government or others, to reveal the contents of the videoconferences without the users' consent.

13. Zoom's privacy violations and security breaches quickly commanded the attention of 27 state attorneys general and the Federal Bureau of Investigation ("F.B.I."). On March 30, 2020, the New York Attorney General sent a letter to Zoom expressing concerns over and inquiring about its data-privacy and security practices. And on March 31, 2020, the

---

[5] Joseph Cox, *Zoom iOS App Sends Data to Facebook Even If You Don't Have a Facebook Account*, VICE, Mar. 26, 2020, *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 May 11, 2020) (the "*Vice* Report").

[6] Taylor Lorenz & Davey Alba, *"Zoombombing" Becomes a Dangerous Organized Effort*, THE NEW YORK TIMES, Apr. 3, 2020 (the "*Times* Zoombombing Report"); Aaron Krollik & Natasha Singer, *A Feature on Zoom Secretly Displayed Data From People's LinkedIn Profiles*, THE NEW YORK TIMES, Apr. 2, 2020 (the "*Times* LinkedIn Report").

[7] Drew Harwell, *Everybody Seems to Be Using Zoom. But Its Security Flaws Could Leave Users at Risk*, THE WASHINGTON POST, Apr. 2, 2020 (the "*Post* Report").

[8] Aaron Tilley & Robert McMillan, *Zoom CEO: "I Really Messed Up" on Video Platform's Security*, THE WALL STREET JOURNAL, Apr. 4, 2020 (the "*WSJ* Report").

[9] Micah Lee & Yael Grauer, *Zoom Meetings Aren't End-to-End Encrypted, Despite Misleading Marketing*, THE INTERCEPT, Mar. 31, 2020, *available a*t https://theintercept.com/2020/03/31/zoom-meeting-encryption/ (last visited May 11, 2020).

F.B.I. issued a warning singling out Zoom based on "multiple reports of conferences being disrupted by pornographic and/or hate images and threatening language." *See Post* Report.

14. While millions of consumers and thousands of businesses and government agencies continue to rely on Zoom to conduct their business during the COVID-19 pandemic, the data-privacy violations and security vulnerabilities at Zoom remain unremedied.

15. By bringing this class action on behalf of themselves and other Zoom users, Plaintiffs seek (a) damages for Zoom's violations of their privacy rights and its unfair, unlawful, and deceptive business practices; and (b) restitution and injunctive relief prohibiting Zoom from continuing its unfair, unlawful, and deceptive business practices.

PARTIES

I. Plaintiffs Saint Paulus Lutheran Church and Heddi N. Cundle

A. Saint Paulus Lutheran Church

16. Plaintiff Saint Paulus Lutheran Church is an Evangelical Lutheran church located at 1541 Polk Street, San Francisco, California. Founded in 1867, Saint Paulus has been serving countless congregants, including the homeless, the marginalized, and the underserved, in San Francisco for over 150 years. The Reverend Daniel Solberg has served as the eighth Pastor of Saint Paulus Lutheran Church since November of 1999. Saint Paulus is a citizen of California.

17. In Saint Paulus's long history, it survived the Great Earthquake and Fire of 1906, the social and cultural turmoil of the 1960s–70s, and a 1995 fire that destroyed its 103-year-old cathedral building. Never did Saint Paulus imagine falling prey to Zoom's deceptive business practices and sex-offenders' depraved hacking during this unprecedented COVID-19 pandemic.

18. To conduct its weekly bible-studies class in compliance with the State's stay-at-home order, Ms. Cundle registered an account with Zoom on behalf of Saint Paulus using an Apple computer on March 17, 2020. Beginning on March 23, 2020, Saint Paulus paid a monthly fee for its Zoom account. Through Ms. Cundle and congregants, Saint Paulus has

used and accessed Zoom since March 25, 2020.

19. Saint Paulus was not aware, and did not understand, that Zoom would share Saint Paulus's private information with third parties, including Facebook. Nor was it aware that Zoom would allow third parties, like Facebook, to access Saint Paulus's private information and combine it with content and information from other sources to create a unique identifier or profile of Saint Paulus for purposes of advertisement.

20. In fact, Saint Paulus registered with Zoom as a user and used Zoom's services in reliance on Zoom's promises that (a) Zoom does not sell users' data; (b) Zoom takes privacy seriously and adequately protects users' personal information; and (c) Zoom's videoconferences are secured with end-to-end encryption and are protected by passwords and other security measures.

B. Heddi N. Cundle

21. Plaintiff Heddi N. Cundle is an administrator at Saint Paulus. She organizes Saint Paulus's weekly bible-study classes. Ms. Cundle is a citizen of California.

22. Ms. Cundle has registered an account with Zoom on behalf of Saint Paulus using an Apple computer at work. She has also registered another account with Zoom for personal use, using her personal email address and personal laptop computer. She has downloaded and installed the iOS version of the Zoom app using her personal Apple iPhone. She has used and accessed Zoom for both work and personal purposes.

23. Ms. Cundle was not aware, and did not understand, that Zoom would share her personal information with third parties, including Facebook. Nor was she aware that Zoom would allow third parties, like Facebook, to access her personal information and combine it with content and information from other sources to create a unique identifier or profile of her for purposes of advertisement.

24. In fact, Ms. Cundle registered with Zoom as a user and used Zoom's services in reliance on Zoom's promises that (a) Zoom does not sell users' data; (b) Zoom takes privacy seriously and adequately protects users' personal information; and (c) Zoom's

videoconferences are secured with end-to-end encryption and are protected by passwords and other security measures.

II. Defendant Zoom Video Communications, Inc.

25. Defendant Zoom Video Communications, Inc. is a Delaware corporation with its principal place of business in San Jose, California. Zoom was founded in 2011 and became a public company in April 2019. Today, Zoom employs a staff of over 1,700 and generates hundreds of millions of dollars in annual revenue.

26. Zoom provides video-communication services. The demand for Zoom's services has exploded in the wake of the COVID-19 pandemic while hundreds of millions of Americans are under orders to stay at home. As a result of the explosion of user demand, Zoom's stock price skyrocketed in recent months. On April 3, 2020, Zoom's stock closed at above $120 per share — nearly doubling its closing price at the beginning of 2020.

JURISDICTION AND VENUE

27. This Court has subject-matter jurisdiction under the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2). The matter in controversy, exclusive of interest and costs, exceeds the sum or value of $5,000,000, and members of the Class are citizens of different states from Zoom.

28. This Court has personal jurisdiction over Zoom because it maintains headquarters in San Jose — within the County of Santa Clara, over which this District presides. Zoom regularly conducts business in this District.

29. Venue is proper in this Court under 28 U.S.C. § 1391 because (a) Zoom transacts business in this District; (b) substantial events and transactions giving rise to this action took place in this District; and (c) many members of the Class reside in this District.

INTRADISTRICT ASSIGNMENT

30. In compliance with Local Rule 3-2(b), Plaintiffs request that this action be assigned to the San Jose Division of this District because a substantial part of the events or conduct giving rise to the claims in this action occurred in the County of Santa Clara.

FACTUAL ALLEGATIONS

I. Zoom Targets Consumers, Businesses, and Government Agencies with Promises of Protecting User Privacy and Ensuring Data Security

31. A fast-growing tech company founded in San Jose in 2011, Zoom provides a "video-first communications platform that … connect[s] people through frictionless video, phone, chat, and content sharing and enable[s] face-to-face video experiences for [up to] thousands of people in a single meeting across disparate devices and locations."[10] Zoom generates revenue from the "sale of subscriptions to [its] platform." Zoom Annual Report at 13. As Zoom itself acknowledges, "security and privacy" are among the key factors affecting its growth and revenue. *See id.*

32. Zoom regularly collects from its users a massive volume of personal information, including names, usernames, physical addresses, email addresses, phone numbers, employment information, credit/debit cards, and cookies and pixels (*e.g.*, through the use of Google Analytics and Google Ads). When users visit Zoom's websites, such as zoom.us and zoom.com, Zoom uses "cookies and tracking technologies" to collect valuable personal data from users:

> ***Zoom collects information about you when you visit our marketing websites***, unless you tell us not to by adjusting your cookie setting. We use such things as cookies and tracking technologies from our advertising service provider tools (*e.g.*, Google Ads). Information collected includes Internet protocol (IP) addresses, browser type, Internet service provider (ISP), referrer URL, exit pages, the files viewed on our marketing sites (*e.g.*, HTML pages, graphics, *etc.*), operating system, date/time stamp, and/or clickstream data.
>
> ***We use this information to determine the offers to make for our services, analyze trends on and run the marketing site, and understand users' movements around the marketing site. We also gather information about our visitors, such as location information at the city level (which we get from IP addresses) for tailoring advertising and selecting the language to use to display the website***.

[10] Zoom's 2020 Annual Report filed in Form 10-K on March 20, 2020 with the U.S. Securities and Exchange Commission, at 4, *available at* https://investors.zoom.us/static-files/09a01665-5f33-4007-8e90-de02219886aa (last visited Apr. 6, 2020) ("Zoom Annual Report").

* * *

> ***Zoom does use certain standard advertising tools on our marketing sites which***, provided you have allowed it in your cookie preferences, ***sends personal data to the tool providers***, ***such as Google***.

Zoom Privacy Policy, *available at* https://zoom.us/privacy (last visited Apr. 6, 2020).[11] Even though Zoom concedes that its "use" of personal information "may be considered a 'sale'" within the meaning of the CCPA, Zoom insists that it "is not selling any data."

33. In fact, Zoom boasts its commitment to user privacy:

> ***Privacy is an extremely important topic, and we want you to know that at Zoom, we take it very seriously***. …
>
> - ***We do not sell your personal data***. …
> - ***Zoom collects only the user data that is required to provide you Zoom services***. This includes technical and operational support and service improvement. For example, we collect information such as a user's IP address and OS and device details to deliver the best possible Zoom experience to you regardless of how and from where you join.
> - ***We do not use data we obtain from your use of our services***, including your meetings, ***for any advertising***. We do use data we obtain from you when you visit our marketing websites, such as zoom.us and zoom.com. You have control over your own cookie settings when visiting our marketing websites.

34. Zoom also advertises that it "take[s] security seriously." On its website, Zoom boasts that it "exceed[s] industry standards" in terms of security measures. Zoom further promises that it "is committed to protecting [users'] privacy," and claims that it has "designed policies and controls to safeguard the collection, use, and disclosure of [users'] information." According to Zoom, it "places privacy and security as the highest priority in the lifecycle operations of our communications infrastructure…."

35. With regard to security in videoconferences, Zoom has, in various parts of its website and in its marketing materials, represented that it uses end-to-end (or E2E)

[11] Unless otherwise noted, all emphases are added.

encryption to secure its videoconferences:

> ***Meet securely***
>
> ***End-to-end encryption for all meetings*** ...
>
> * * *
>
> Protect your Meetings
> The following in-meeting security capabilities are available to the meeting host:
> • ***Secure a meeting with end-to-end encryption***
>
> * * *
>
> Enables HIPPA, 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.

36. As noted in the *Intercept* Report, Zoom's bald and unequivocal promise of end-to-end encryption is important to consumers because it is "widely understood as the most private form of internet communication." An end-to-end encrypted videoconference means that "the video and audio content [are] encrypted in such a way that only the participants in the meeting have the ability to decrypt it." *See Intercept* Report. In other words, only the videoconference participants themselves — not Zoom or any other third parties — have access to the contents of their videoconferences.

37. As detailed below, however, Zoom's promise of end-to-end encryption is false. In fact, in response to the *Intercept*'s revelation of its false promises regarding end-to-end encryption, a Zoom spokesperson admitted in late March 2020 that "[c]urrently, it is not possible to enable E2E encryption for Zoom video meetings" due to the design and operation of Zoom's platform.

38. In addition to end-to-end encryption, Zoom also boasts its capacity to "secure" a meeting "with password" using its "[r]ole-based user security":

> Client Application
> Role-based user security
> The following pre-meeting security capabilities are available to the meeting host:
> • ***Enable an end-to-end (E2E) encrypted meeting***

> • Secure log-in using standard ***username and password*** … sign-on
> • Start ***a secured meeting with password***
> • Schedule a secured meeting with password
>
> * * *
>
> Meeting Security
> Role-based user security
> The following in-meeting security capabilities are available to the meeting host:
> • ***Secure a meeting with E2E encryption***
> …
> • ***Expel a participant or all participants***
> • End a meeting
> • ***Lock a meeting***
> …
> • Mute/unmute a participant or all participants
> …
> • Enable/disable a participant or all participants to record …

See Zoom Security Guide, *available at* https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf (last visited Apr. 6, 2020). As detailed below, however, Zoom's representations regarding security of its videoconferences are false because "'Zoombombing' … by uninvited participants ha[s] become frequent." *See Times* Zoombombing Report.

39. Yet, Zoom profits from these false promises of data protection and security. Before the COVID-19 outbreak, Zoom induced — using these false promises — millions of consumers, as well as business and government agencies, to register for its services. The volume of Zoom's business generated an annual revenue of $622.7 million in the fiscal year of 2020 (ending January 31, 2020). Zoom Annual Report at 38. In April 2019, Zoom issued 20 million shares of its common stock at $36 per share in a successful initial public offering.

40. Since the outbreak of the COVID-19 pandemic, the demand for Zoom's services has skyrocketed:

> Zoom was used by more than 200 million callers [in March 2020], up from 10 million in December [2019], and is used in more than 90,000 schools across 20 countries …. More than 5 million people in the United States used Zoom's mobile apps on [April 1, 2020], five times more than a month ago, dwarfing the competition of its top rivals, including Skype, Slack, Google Hangouts and Microsoft Teams ….

See Post Report. According to the app data firm SensorTower, "first-time installs of the videoconferencing company's mobile app rose by 1,126 percent in March to more than 76 million, up from just 6.2 million in February." *Times* Zoombombing Report.

41. Likewise, Zoom's stock price skyrocketed — trading at one point at a high of $164.94 per share (on March 23, 2020). Today, Zoom amasses over $30 billion in market capitalization. Zoom's exponential growth of market capitalization is predicated upon users' trust in its promises of data privacy and security. But these promises are false.

II. Zoom Broke Its Promises of Data Privacy and Security

A. Zoom Collected and Disclosed Users' Personal Information Without Authorization or Consent

42. Zoom's promises of data privacy and security are false. As revealed in the *Vice* Report, the iOS version of Zoom's mobile app sent users' personal information to Facebook for use in targeted advertising, ***without first notifying the users or obtaining their consent***. Zoom provided users' personal information to Facebook even for users who do not have Facebook accounts. *See Vice* Report.

43. According to the *Vice* Report, upon downloading and opening the app, Zoom would connect to Facebook's Graph API ("application program interface") — a primary way to get data into and out of the Facebook platform.

44. When a Zoom user opens the iOS version of the Zoom app, Zoom would notify Facebook that the user has opened the app and identify the user's device (*i.e.*, the model), time zone, physical location, and telephone carrier. Such personal information then generates a unique identifier that enables companies like Facebook to target the user with advertisements. Advertisers then use the identifier to track data so that they can deliver customized advertising. The identifier is also used for tracking and identifying a user, allowing whoever is tracking it to identify a user when he or she interacts with or responds to advertisements. An identifier is similar to a cookie: it allows advertisers to know that a specific user is viewing a specific publication so that it can serve an advertisement targeting that user. Such identifiers are extremely valuable in the online advertising industry.

45. According to one privacy-protection expert, Zoom's practices of data collection and data sharing are "shocking," because "[t]here is nothing in [Zoom's] privacy policy that addresses that." *See Vice* Report.

46. Aside from the lack of any notice, Zoom's data-sharing activity was not visible to users because they can only see the Zoom app interface. Thus, Zoom provides users ***no opportunity to consent to or opt out of*** Zoom's data-sharing with Facebook. Zoom's lack of disclosure and failure to provide an opportunity to opt out is particularly glaring in light of Facebook's own admonition to developers like Zoom to give notice:

> Facebook told [*Vice*] it ***requires developers to be transparent with users about the data their apps send to Facebook***. Facebook's terms say "If you use our pixels or SDK [(software development kits)], you further represent and warrant that you have provided ***robust and sufficiently prominent notice to users regarding the Customer Data collection***, ***sharing and usage***," and specifically for apps, "***that third parties, including Facebook, may collect or receive information from your app and other apps and use that information to provide measurement services and targeted ads***."

See Vice Report.

47. Indeed, after being confronted with *Vice*'s findings, "***Zoom confirmed the data collection*** in a statement to [*Vice*]":

> We originally implemented the 'Login with Facebook' feature using the Facebook SDK in order to provide our users with another convenient way to access our platform. However, ***we were recently made aware that the Facebook SDK was collecting unnecessary device data*** [as identified by *Vice*.] ...
>
> To address this, in the next few days, we will be removing the Facebook SDK and reconfiguring the feature so that users will still be able to login with Facebook via their browser. Users 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.

See Vice Report.

48. Despite admitting to the "oversight" and purporting to release a new version of the Zoom app (as of March 27, 2020) as a remedy, the harm to Plaintiffs and other Class

members, as well as the violations of their privacy, have occurred and continue to occur because, even assuming no unauthorized disclosure of personal information is made through the new version, the previous version of the app remains operational. Moreover, Zoom failed to mandate the use of the new version of the app. Nor did Zoom do anything to rectify its previous egregious violations of users' privacy rights.

49. Upon information and belief, Zoom provides users' personal information to other third parties, in addition to Facebook, for unauthorized purposes, including use in targeted advertising.

50. Plaintiffs and other reasonable Zoom users did not know that when they signed up to use Zoom's services that Zoom would share their personal information with third parties for the purpose and in the manner set forth above, and that their privacy rights would be violated. Had Plaintiffs and other users known about Zoom's data-sharing practices, they would not have signed up with Zoom and would not have used Zoom's services.

51. Zoom's unlawful disclosure of users' personal information is not limited to Facebook. According to the *Times* LinkedIn Report, Zoom used data-mining tools to collect users' personal information without authorization, then used the personal information to match the users' LinkedIn profiles:

> For Americans sheltering at home during the coronavirus pandemic, the Zoom videoconferencing platform has become a lifeline, enabling millions of people to easily keep in touch with family members, friends, students, teachers and work colleagues.
>
> But what many people may not know is that, until Thursday, ***a data-mining feature on Zoom allowed some participants to surreptitiously have access to LinkedIn profile data about other users — without Zoom asking for their permission during the meeting or even notifying them that someone else was snooping on them***.
>
> ***The undisclosed data mining adds to growing concerns about Zoom's business practices*** at a moment when public schools, health providers, employers, fitness trainers, prime ministers and queer dance parties are embracing the platform.

> An analysis by *The New York Times* found that when people signed in to a meeting, ***Zoom's software automatically sent their names and email addresses to a company system it used to match them with their LinkedIn profiles***.

52. As *The New York Times* noted, "neither Zoom's privacy policy nor its terms of service specifically disclosed that Zoom could covertly display meeting participants' LinkedIn data to other users — or that it might communicate the names and email addresses of participants in private Zoom meetings to LinkedIn." *Times* LinkedIn Report. In fact, "user instructions on Zoom suggested just the opposite: that meeting attendees may control who sees their real names." *Id*. Accordingly, "***privacy experts criticized Zoom for making the data-mining tools available during meetings without alerting participants as they were being subjected to them***." *Id*.

53. Although Zoom claims that, after the revelations made in the *Times* LinkedIn Report, it discontinued the practice of mining and revealing users' LinkedIn information without authorization, Zoom has done nothing to rectify its past violations of users' privacy and unlawful practices of unauthorized data mining, collection, and disclosure.

B. Zoom Failed to Implement Adequate Security Protocols Jeopardizing Users' Account Security

54. Zoom's inadequate security practices were exposed again on April 15, 2020, when an information security and technology news publication, *BleepingComputer*, reported that hackers were selling half a million Zoom account in the dark web:[12]

> An exploit for a zero-day remote code execution vulnerability affecting the Zoom Windows client is currently being sold for $500,000, together with one designed to abused a bug in the video conferencing platform's macOS client.
>
> * * *
>
> As *BleepingComputer* reported on Monday, ***more than 500,000 Zoom accounts are being sold on hacker forums and on the dark web for less than a penny each***, and, in some cases***, also given away***

[12] Sergiu Gatlan, *Exploit for Zoom Windows Zero-Day Being Sold for $500,000*, BLEEPINGCOMPUTER, Apr. 15, 2020, *available at* https://www.bleepingcomputer.com/news/security/exploit-for-zoom-windows-zero-day-being-sold-for-500-000/ (last visited May 11, 2020).

for free to be used in zoom-bombing pranks and various other malicious activities.

55. The information relating to these half a million Zoom accounts was published and exchanged online without Zoom users' consent or knowledge. Zoom is responsible for violating users' privacy due to its failure to implement adequate security protocols and review procedures that could have and should have prevented the hacking of these accounts.

56. As a result of Zoom's failures, Plaintiffs and other Class members are subjected to increased risks of imminent harm to their privacy rights.

C. Zoom Failed to Maintain Adequate Measures to Protect Data Privacy and Ensure Videoconference Security

57. On Zoom's websites and in its marketing materials, Zoom has repeatedly touted the security of its videoconferences — that they are protected by passwords and end-to-end encryption. In reality, however, Zoom's videoconferences are vulnerable to hacking — as evident in the increased frequency of Zoombombing. Worse, as Zoom admitted in its recent disclosures, ***Zoom lacks the capacity to implement end-to-end encryption***.

58. As noted in the *Intercept* Report, Zoom "claims to implement end-to-end encryption, widely understood as the most private form of internet communication, protecting conversations from all outside parties." But this is false. In fact, "Zoom is using its own definition of the term, ***one that lets Zoom itself access unencrypted video and audio from meetings***."

59. When confronted by the *Intercept* regarding this false representation, Zoom all but admitted that it lacks the technology to protect videoconferences with end-to-end encryption:

> But when reached for comment about whether video meetings are actually end-to-end encrypted, 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."

> The encryption that Zoom uses to protect meetings is TLS, the same technology that web servers use to secure HTTPS websites. This means that the connection between the Zoom app running on a user's computer or phone and Zoom's server is encrypted in the same way the connection between your web browser and this article (on https://theintercept.com) is encrypted. ***This is known as transport encryption, which is different from end-to-end encryption because the Zoom service itself can access the unencrypted video and audio content of Zoom meetings***. So when you have a Zoom meeting, the video and audio content will stay private from anyone spying on your Wi-Fi, but it won't stay private from the company. (In a statement, Zoom said it does not directly access, mine, or sell user data; more below.)
>
> ...
>
> "***When we use the phrase 'End to End' in our other literature, it is in reference to the connection being encrypted from Zoom end point to Zoom end point***," the Zoom spokesperson wrote, ***apparently referring to Zoom servers as "end points" even though they sit between Zoom clients***. "The content is not decrypted as it transfers across the Zoom cloud" through the networking between these machines.

See Intercept Report.

60. According to one cryptographer, Professor Matthew D. Green of Johns Hopkins University's Department of Computer Science, Zoom is twisting the common meaning of "end-to-end" in a "***dishonest way***":

> "They're a little bit fuzzy about what's end-to-end encrypted," Green said of Zoom. "I think they're doing this in a slightly dishonest way. It would be nice if they just came clean."

See id.

61. Caught red-handed, Zoom apologized on April 1, 2020 "in a blog post for the 'discrepancy between the commonly accepted definition of end-to-end encryption and how [Zoom was] using it." *Post* Report.

62. Zoom's dishonesty is particularly glaring in light of the fact that several of Zoom's competitors, including Apple FaceTime and Signal, offer real end-to-end encryption in their videoconferences:

> "If it's all end-to-end encrypted, you need to add some extra mechanisms to make sure you can do that kind of 'who's talking' switch, and you can do it in a way that doesn't leak a lot of information. You have to push that logic out to the endpoints," he told *The Intercept*. This isn't impossible,

> though, Green said, as demonstrated by Apple's FaceTime, which allows group video conferencing that's end-to-end encrypted. "***It's doable. It's just not easy***."

See Intercept Report.

63. Thus, it is not that Zoom could not have fulfilled its promise of end-to-end encryption. It is that Zoom made a conscious decision to make the false promise — knowing that it lacked the technology to keep the promise.

64. Moreover, Zoom has done nothing, aside from issuing empty words in a blog-posted "apology," to improve security in its videoconferences and to rectify past security breaches.

65. Likewise, as discussed above, Zoom's marketing materials provide users with a false sense of security regarding its videoconferences.

66. But Zoom's videoconferences are anything but secure. In recent weeks, Zoombombing has become a daily element of Zoom's videoconferences:

> [Zoom] has faced added pressure from the rise of "zoombombing" raids, in which anonymous trolls barge into unlocked Zoom meetings, shouting profane insults and racist slurs. Videos of the raids, some of which have been removed by YouTube for violating hate-speech policies, show giggling trolls posting pornography into online grade-school lessons, pulling their pants down in front of company conference calls, and dancing with bottles of bourbon in what appeared to be an online Alcoholics Anonymous meeting.

See Post Report.

67. By failing to properly maintain security in its videoconferences, Zoom has enabled hackers and pranksters to perpetrate online abuse on a massive scale:

> An analysis by *The New York Times* found 153 Instagram accounts, dozens of Twitter accounts and private chats, and several active message boards on Reddit and 4Chan where thousands of people had gathered to organize Zoom harassment campaigns, sharing meeting passwords and plans for sowing chaos in public and private meetings. (Since this article's publication, Reddit has shut down the message boards where Zoom raids were discussed.)
>
> Zoom raiders often employ shocking imagery, racial epithets and profanity to derail video conferences. Though a meeting organizer can remove a participant at any time, the perpetrators of these attacks can be hard to

> identify; there may be several in a single call, and they can appear to jump from one alias to another.

See Times Zoombombing Report.

68. "The frequency and reach of the incidents on Zoom prompted the F.B.I. to issue a warning on [March 31, 2020], singling out the [Zoom] app and stating that it had 'received multiple reports of conferences being disrupted by pornographic or hate images and threatening language' nationwide." *Id.*

69. In addition to the F.B.I., other state and federal authorities also intervened. The attorneys generals of 27 states, including New York, have raised questions about privacy issues and demanded that Zoom cooperate with them in multiple investigations. *See WSJ* Report. Senator Richard Blumenthal of Connecticut wrote a letter to Zoom on March 31, 2020 demanding answers about Zoom's "'troubling history of software design practices and security lapses.'" *Id.* Senator Blumenthal expressed grave concerns over Zoom's privacy violations and security breaches:

> ***The millions of Americans*** now unexpectedly attending school, celebrating birthdays, seeking medical help, and sharing evening drinks with friends over Zoom during the coronavirus pandemic, … ***should not have to add privacy and cybersecurity fears to their ever-growing list of worries***.

Id. (internal quotation marks omitted).

70. In its public disclosures, Zoom admits that its security is inadequate. Zoom's founder and Chief Executive Officer, Eric Yuan, told *The Wall Street Journal*: "***I really messed up***" on Zoom's security. *See id.* But Zoom has done little to improve security. While Mr. Yuan promised to develop "an option for end-to-end encryption to safeguard conversations, … [the] feature won't be ready for a few months." *Id.*

71. While Zoom continues to make empty, false promises, American consumers are left to deal with the privacy violations and security breaches inflicted by Zoom and, in Senator Blumenthal's words, "add[ing] privacy and cybersecurity fears to their ever-growing list of worries." *Id.*

72. On behalf of these American consumers, Plaintiffs bring this action for damages and injunctive relief to rectify Zoom's misconduct.

III. Plaintiffs' Experience with Zoom and Zoombombing

A. Saint Paulus and Ms. Cundle Registered Accounts with Zoom in Reliance on Its False Representations of Data Protection and Conference Security

73. Saint Paulus has been conducting a weekly bible-study class for two decades. The class, typically running for two hours, is open to the public and is usually attended by senior congregants (over 65 years old).

74. Following California's March 4, 2020 declaration of a state of emergency as a result of the COVID-19 pandemic, Saint Paulus began searching for alternative meeting venues to conduct its weekly bible-study classes. Based on Zoom's advertisements of a user-friendly and secure platform, Zoom videoconferencing stood out as a prime candidate for conducting online classes.

75. On March 17, 2020, Ms. Cundle, serving as Saint Paulus's administrator, registered an account with Zoom, using her work email address. On March 23, 2020, following the March 19, 2020 issuance of the statewide Executive Order N-33-20 (directing all California residents to stay at home), Saint Paulus upgraded its Zoom account to "premium" status by paying a monthly fee of $14.99. Ms. Cundle downloaded Zoom's software onto an Apple desktop computer at Saint Paulus.

76. Ms. Cundle also registered another account for her personal use. She downloaded Zoom's software using her personal laptop computer. She downloaded and installed the iOS version of the Zoom app using her personal Apple iPhone.

77. At the time when Saint Paulus and Ms. Cundle registered their accounts with Zoom, Saint Paulus and Ms. Cundle were not aware, and did not understand, that Zoom would share Saint Paulus's personal information with third parties, including Facebook. Nor was Saint Paulus or Ms. Cundle aware that Zoom would allow third parties, like Facebook, to access its personal information and combine it with content and information from other

sources to create a unique identifier or profile of Saint Paulus for purposes of advertisement.

78. In fact, Saint Paulus and Ms. Cundle registered with Zoom as users and used Zoom's services in reliance on Zoom's promises that (a) Zoom does not sell users' data; (b) Zoom takes privacy seriously and adequately protects users' personal information; and (c) Zoom's videoconferences are secured with end-to-end encryption and are protected by passwords and other security measures.

B. Saint Paulus, Its Congregants, and Ms. Cundle Became Victims of Zoombombing

79. Starting on March 25, 2020, Saint Paulus conducted its weekly two-hour-long bible-study class using Zoom videoconference. Ms. Cundle served as an organizer for these Zoom videoconferences. To that end, she set up the Zoom videoconferences before each class, following Zoom's instructions. Based on Zoom's representations, she understood that the videoconferences would be protected by passwords, and that, as the organizer, she would have the ability to control the videoconferences, including being able to eject any participant from the videoconferences.

80. For the May 6, 2020 class (starting at 12:00 p.m. Pacific Time), Ms. Cundle set up a password-protected Zoom videoconference, following Zoom's instructions.

81. The May 6, 2020 class was held on Zoom with nine participants, including Ms. Cundle as the organizer. The class was uneventful until approximately 42 minutes into the class, when an intruder with the name "Christine (iPad)" hacked into the videoconference — despite Zoom's advertisement of password protection.

82. Immediately following the break-in, pornographic video footages began to run on all participants' computers in a full-screen mode and with loud audio. Ms. Cundle and the other participants were forced to view various footages of adults performing sexual acts with each other and on infants and on young children. Some footages involved physical abuse of children, in addition to sexual acts. Ms. Cundle and the other participants were unable to minimize or close the video screen. Nor were they able to use any of the Zoom functions to refuse viewing the pornographic video or eject the intruder (Christine (iPad))

from the Zoom meeting. None of the organizer functions advertised by Zoom worked.

83. After attempting to avoid the pornographic video and eject the intruder — to no avail — Ms. Cundle and the other participants logged off the meeting and logged back on, hoping to be rid of the intruder.

84. But the intruder returned immediately to the new bible-study session. Pornographic video footages reappeared on every participant's computer — again on full screen mode with loud audio. The footages again involved adults engaging in sexual acts and performing sexual acts on infants and young children. The footages also showed physical abuse of children, as well as defecation and other deviant acts.

85. The depravity of the video footages was beyond description. Ms. Cundle and the other participants were traumatized and deeply disturbed.

86. Ms. Cundle and the other participants again attempted to use Zoom functions to eject the intruder from the bible-study class. But all efforts failed.

87. Ms. Cundle had no choice but to terminate the bible-study class before 1:00 p.m. on May 6, 2020.

C. Zoom Rejected Saint Paulus's Repeated Pleas to Improve Security

88. Immediately following the traumatizing incident, Ms. Cundle sought help from Zoom by contacting Zoom online and by telephone. Ms. Cundle sent an online request to Zoom, reporting the incident and demanding action to remedy the situation and prevent further Zoombombing.

89. On May 6, 2020, Ms. Cundle reported this Zoombombing incident to Pastor Solberg and the Saint Paulus Lutheran Church Council. Deeply concerned about this disturbing incident, Pastor Solberg and the Council immediately worked with Ms. Cundle to remedy the situation.

90. In an email response dated May 6, 2020, Zoom's Trust & Safety department stated that it had identified the intruder and blocked the intruder "from joining future meetings using the same Zoom software." But Zoom refused to take any further action to

remedy the situation or to improve the security of its videoconferences. Shockingly, Zoom admitted that the intruder was "a known serial offender who disrupts open meetings by showing the same video," and had "been reported multiple times to the authorities":

> We identified in your meeting ***a known serial offender who disrupts open meetings by showing the same video***, and which ***has been reported multiple times to the authorities***. This intruder has the following identifying information:
>
> Christine (iPad)
>
> The report ID for Christine (iPad) is 71731955. You can use this number when you submit your report to link both reports.

It is baffling, to say the least, how Zoom failed to protect Saint Paulus's bible-study class from a "serial offender" who has been "reported multiple times to the authorities."

91. Dissatisfied with this, Ms. Cundle also reached out to Zoom's management for help. To that end, Ms. Cundle contacted Zoom's Deputy General Counsel and Chief Compliance and Ethics Officer, Lynn Haaland, Zoom's Chief Information Security Officer, Richard Farley, and Zoom's Chief Executive Officer, Eric S. Yuan. Neither Haaland nor Farley, however, offered any help to rectify the situation or take action to ensure security. Yuan failed to respond to Ms. Cundle's emails.

92. On behalf of Saint Paulus, Ms. Cundle reported the incidents to law-enforcement agencies, including the F.B.I. and the San Francisco Police Department.

FRAUDULENT CONCEALMENT AND TOLLING

93. The applicable statutes of limitations are tolled because Zoom knowingly and actively concealed the facts alleged above. Until the revelations made in March 2020, Plaintiffs and the Class members did not know and could not have known of the information essential to the pursuit of these claims through no fault of their own and not due to any lack of diligence on their part.

CLASS ACTION ALLEGATIONS

94. Plaintiffs bring this action as a class action under Rule 23 of the Federal Rules of Civil Procedure, on behalf of a proposed class (the "Class"), defined as:

All persons in the United States who used Zoom during the applicable limitations period.

95. Excluded from the Class are any entities, including Zoom, in which Zoom or its subsidiaries or affiliates have a controlling interest, Zoom's officers, agents and employees, the judicial officer to whom this action is assigned and any member of the Court's staff and immediate families, as well as claims for personal injury, wrongful death, and emotional distress.

96. **Numerosity Under Rule 23(a)(1)**. The members of the Class are so numerous that joinder of all members would be impracticable. Based on information and belief, Plaintiffs allege that the Class includes millions of members.

97. **Commonality and Predominance Under Rule 23(a)(2) and 23(b)(3)**. This action involves common questions of law or fact, which predominate over any questions affecting individual Class members, including:

(a) whether Zoom shared the personal information of Plaintiffs and other Class members with third parties without their authorization or consent;

(b) whether Zoom violated Plaintiffs' and Class members' privacy rights;

(c) whether Zoom intruded upon Plaintiffs' and the Class members' seclusion;

(d) whether Zoom acted negligently;

(e) whether Plaintiffs and other Class members formed implied contracts with Zoom;

(f) whether Zoom breached implied contracts with Plaintiffs and the Class members and breached the implied covenant of good faith and fair dealing;

(g) whether Zoom violated the CCPA;

(h) whether Zoom violated the CLRA;

(i) whether Zoom violated the UCL;

(j) whether Plaintiffs and the Class members were harmed as a result of

Zoom's conduct;

(k) whether Plaintiffs and the Class members are entitled to actual, statutory, or other forms of damages or any other monetary relief; and

(l) whether Plaintiffs and the Class members are entitled to equitable relief.

98. Plaintiffs' claims are typical of the members of the Class as all members of the Class are similarly affected by Zoom's actionable conduct. Zoom's conduct that gave rise to Plaintiffs' claims is the same for all members of the Class.

99. Zoom engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs and on behalf of the other Class members. Similar or identical statutory and common-law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

100. **Typicality Under Rule 23(a)(3)**. Plaintiffs' claims are typical of the claims of the other Class members because, among other things, (a) Plaintiffs and the other Class members provided personal information to Zoom; and (b) in its uniform misconduct alleged above, Zoom shared the personal information of Plaintiffs and other Class members without their authorization or consent. Plaintiffs and other Class members are advancing the same claims and based on the same legal theories. There are no defenses that are unique to Plaintiffs.

101. **Adequacy of Representation Under Rule 23(a)(4)**. Plaintiffs are adequate representatives of the Class because (a) their interests do not conflict with the interests of the other Class members it seeks to represent; (b) they have retained counsel competent and experienced in complex class action litigation, including data-privacy litigation; (c) they will prosecute this action vigorously; and (d) they have no interests that are contrary to or in conflict with the interests of other Class members.

102. **Superiority Under Rule 23(b)(3)**. A class action is superior to other

available methods for the fair and efficient adjudication of this controversy because joinder of all the members of the Class is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There should be no difficulty in managing this action as a class action.

103. Class certification is also appropriate under Rule 23(b)(2) because Zoom has acted or has refused to act on grounds generally applicable to the Class, so that corresponding declaratory relief is appropriate to the Classes as a whole.

104. California law applies to the claims asserted in this complaint because:

- Zoom is headquartered in California;
- all of Zoom's key decisions and a substantial part of its operations emanate from California;
- a substantial number of the Class members reside in California;
- California has a strong interest in preventing corporations headquartered in the state from engaging in unfair, unlawful, and deceptive business practices; and
- California has a strong interest in providing redress for its citizens for Zoom's illegal conduct.

CAUSES OF ACTION

Count I
Negligence

105. Plaintiffs repeats and incorporate by reference each and every allegation set forth above, as though fully set forth herein.

106. Zoom owed a duty to Plaintiffs and the other Class members to exercise reasonable care in (a) using their personal information in compliance with all applicable law and the terms of Zoom's privacy policy; (b) safeguarding their personal information in its possession; and (c) ensuring security in Zoom's videoconferences. To fulfill this duty, Zoom is obligated to implement and maintain adequate security measures to protect its users'

personal information and to avoid disclosure of its users' personal information to any third parties without their knowledge and consent.

107. Plaintiffs and the Class members used Zoom's services in reliance on its exercise of due care and fulfillment of its duties.

108. Zoom, however, breached its duties by, among other things:

- disclosing Plaintiffs' and other Class members' personal information to unauthorized third parties, including Facebook;
- allowing third parties to access the personal information of Plaintiffs and other Class members;
- failing to implement and maintain adequate security measures to safeguard users' personal information;
- failing to timely notify Plaintiffs and other Class members of the unlawful disclosure of their personal information; and
- failing to maintain adequate security and proper encryption in Zoom's videoconferences.

109. Zoom's misconduct is inconsistent with industry regulations and standards.

110. Plaintiffs and other Class members did not contribute to Zoom's misconduct.

111. The harm inflicted upon Plaintiffs and other Class members is reasonably foreseeable to Zoom.

112. As a direct and proximate result of Zoom's misconduct, Plaintiffs and other Class members have suffered damages relating to, among other things, loss of privacy and emotional distress.

Count II
Breach of Implied Contract

113. Plaintiffs repeat and incorporate by reference each and every allegation set forth above, as though fully set forth herein.

114. To generate revenues, attract advertisers, and increase market share, Zoom offered Plaintiffs and other Class members to use its services by creating Zoom accounts,

which require the provision of confidential, sensitive personal information.

115. Accepting Zoom's offer, Plaintiffs and other Class members obtained user accounts from Zoom and provided Zoom with confidential, sensitive personal information.

116. By becoming users of Zoom's services, Plaintiffs and other Class members entered into implied contracts with Zoom, under which Zoom, for its own benefit, obtained from Plaintiffs and other Class members their confidential, sensitive personal information, as well as money. In exchange, Zoom agreed, at least implicitly, to (a) safeguard such information against unauthorized disclosure, access, or use; (b) timely notify Plaintiffs and other Class members of any unauthorized disclosure of, access to, or use of such information; and (c) maintain adequate security and proper encryption in Zoom's videoconferences.

117. Without such an implicit agreement by Zoom, Plaintiffs and other Class members would not have entrusted their personal information to Zoom or paid for its services. Instead, Plaintiffs and other Class members would have chosen an alternative videoconference platform that would refrain from sharing their personal information with undisclosed and unauthorized third parties and maintain adequate security and proper encryption in videoconferences.

118. Plaintiffs and other Class members fully performed their obligations under the implied contract with Zoom.

119. Zoom, however, breached the implied contracts it made with Plaintiffs and other Class members by, among other things:

- disclosing Plaintiffs' and other Class members' personal information to unauthorized third parties, including Facebook;
- allowing third parties to access the personal information of Plaintiffs and other Class members;
- failing to implement and maintain adequate security measures to safeguard users' personal information;
- failing to timely notify Plaintiffs and other Class members of the unlawful

disclosure of their personal information; and

- failing to maintain adequate security and proper encryption in Zoom's videoconferences.

120. By breaching its implied contracts with Plaintiffs and other Class members, Zoom is not entitled to retain the benefits it received.

121. As a direct and proximate result of Zoom's breaches of the implied contracts, Plaintiffs and other Class members have suffered actual losses and damages.

Count III
Breach of the Implied Covenant of Good Faith and Fair Dealing

122. Plaintiffs repeat and incorporate by reference each and every allegation set forth above, as though fully set forth herein.

123. There is a covenant of good faith and fair dealing implied in every implied contract. This implied covenant requires each contracting party to refrain from doing anything to injure the right of the other to receive the benefits of the agreement. To fulfill its covenant, a party must give at least as much consideration to the interests of the other party as it gives to its own interests.

124. Under the implied covenant of good faith and fair dealing, Zoom is obligated to, at a minimum, (a) implement proper procedures to safeguard the personal information of Plaintiffs and other Class members; (b) refrain from disclosing, without authorization or consent, the personal information of Plaintiffs and other Class members to any third parties; (c) promptly and accurately notify Plaintiffs and other Class members of any unauthorized disclosure of, access to, and use of their personal information; and (d) maintain adequate security and proper encryption in Zoom's videoconferences.

125. Zoom breached the implied covenant of good faith and fair dealing by, among other things:

- disclosing Plaintiffs' and other Class members' personal information to unauthorized third parties, including Facebook;
- allowing third parties to access the personal information of Plaintiffs and

other Class members;

- failing to implement and maintain adequate security measures to safeguard users' personal information;
- failing to timely notify Plaintiffs and other Class members of the unlawful disclosure of their personal information; and
- failing to maintain adequate security and proper encryption in Zoom's videoconferences.

126. As a direct and proximate result of Zoom's breaches of the implied covenant of good faith and fair dealing, Plaintiffs and other Class members have suffered actual losses and damages.

Count IV
Unjust Enrichment

127. Plaintiffs repeat and incorporate by reference each and every allegation set forth above, as though fully set forth herein.

128. Zoom has benefited and profited from Plaintiffs' and other Class members' use of its videoconferencing services by obtaining their personal information and money.

129. Zoom, however, failed to provide Plaintiffs and other Class members the services they reasonably expected because Zoom:

- disclosed Plaintiffs' and other Class members' personal information to unauthorized third parties, including Facebook;
- allowed third parties to access the personal information of Plaintiffs and other Class members;
- failed to implement and maintain adequate security measures to safeguard users' personal information;
- failed to timely notify Plaintiffs and other Class members of the unlawful disclosure of their personal information; and
- failed to maintain adequate security and proper encryption in Zoom's videoconferences.

130. Zoom has therefore been unjustly enriched by its retention of the benefits and profits at the expense of Plaintiffs and other Class members. Equity and justice require that Zoom disgorge the benefits and profits.

131. Plaintiffs seek an order directing Zoom to disgorge these benefits and profits and pay restitution to Plaintiffs and other Class members.

Count V
Violation of the California Consumer Privacy Act

132. Plaintiffs repeat and incorporate by reference each and every allegation set forth above, as though fully set forth herein.

133. The CCPA prohibits collection and use of consumers' personal information from collection and use by businesses without consumers' notice and consent.

134. Zoom violated the CCPA by using the personal information of Plaintiffs and other Class members without providing the required notice under the CCPA. *See* CAL. CIV. CODE § 1798.100(b). Zoom did not notify Plaintiffs and the Class members that it was disclosing their personal information to unauthorized parties.

135. Zoom also violated the CCPA by failing to provide notice to Plaintiffs and other Class members of their right to opt out of the disclosure or use of their personal information to third parties. *See* CAL. CIV. CODE § 1798.120(b). Zoom failed to give Plaintiffs and the Class members the opportunity to opt out before sharing their personal information with unauthorized parties.

136. Plaintiffs seek damages on behalf of themselves and the Class, as well as injunctive relief in the form of an order enjoining Zoom from continuing to violate the CCPA.

Count VI
Violation of California's Consumer Legal Remedies Act

137. Plaintiffs repeat and incorporate by reference each and every allegation set forth above, as though fully set forth herein.

138. Plaintiffs and each Class Member are "consumers" under the CLRA, *see* CAL. CIV. CODE § 1761(d).

139. Zoom is a "person" as defined by the CLRA, *see* CAL. CIV. CODE § 1761(c).

140. Zoom's marketing and sale of the Zoom app is the sale of a "good" and "service" to consumers within the meaning of the CLRA, *see* CAL. CIV. CODE §§ 1761(a)–(b), 1770(a).

141. The CLRA protects consumers against unfair and deceptive practices, and is intended to provide an efficient means of securing such protection.

142. As detailed above in paragraphs 26 through 33, Zoom promised to protect data privacy and secure videoconferences. Zoom violated the CLRA by, among other things:

- disclosing Plaintiffs' and other Class members' personal information to unauthorized third parties, including Facebook;
- allowing third parties to access the personal information of Plaintiffs and other Class members;
- failing to implement and maintain adequate security measures to safeguard users' personal information;
- failing to, in a timely manner, (a) investigate the unauthorized disclosures described above, and (b) notify Plaintiffs and other Class members of the unauthorized disclosure of, access to, and use of their personal information; and
- failing to maintain adequate security and proper encryption in Zoom's videoconferences.

143. Zoom's conduct is deceptive and unfair and violates Subsection 1770(a) of the California Civil Code because:

- Zoom represented that its product had characteristics it did not have in violation of Subsection (a)(5);
- Zoom represented its products were of a particular standard, grade, or quality when they were of another in violation of Subsection (a)(7);
- Zoom advertised its services with intent not to sell them as advertised in violation of Subsection (a)(9); and

- Zoom knowingly and intentionally withheld material information from Plaintiffs and the Class members in violation of Subsection (a)(14).

144. Zoom's unfair or deceptive acts and practices were capable of deceiving a substantial portion of the public. Zoom did not disclose the facts of its disclosure of personal information and its lack of capacity to secure videoconferences because it knew that consumers would not use its products or services, and instead would use other products or services, had they known the truth.

145. Zoom had a duty to disclose the truth about its privacy practices and security capabilities because it is in a superior position to know whether, when, and how it discloses users' information to third parties and whether it can ensure security in videoconferences.

146. Plaintiffs and the Class members could not reasonably have been expected to learn or discover Zoom's disclosure of their personal information to unauthorized parties or Zoom's lack of capacity to secure videoconferences.

147. The facts concealed by Zoom are material because a reasonable consumer would have considered them to be important in deciding whether to use Zoom.

148. Plaintiffs and the Class members reasonably expected that Zoom would (a) safeguard their personal information and refrain from disclosing it without their consent; and (b) ensure security in Zoom's videoconferences.

149. Due to Zoom's violations of the CLRA, Plaintiffs and the Class members suffered damages and did not receive the benefit of their bargain with Zoom because they paid for a value of services, either through personal information or a combination of their personal information and money.

150. Plaintiffs and the Class members seek an injunction barring Zoom from disclosing their personal information without their consent and requiring Zoom to ensure security in videoconferences.

Count VII
Violation of the Unfair Competition Law

151. Plaintiffs repeat and incorporate by reference each and every allegation set

forth above, as though fully set forth herein.

152. Zoom engaged in unfair, unlawful, and fraudulent business practices within the meaning of the UCL, CAL. BUS. & PROF. CODE §§ 17200, *et seq*.

153. Zoom collected and stored confidential, sensitive personal information from Plaintiffs and other Class members. Zoom falsely represented to Plaintiffs and other Class members that:

(a) "[w]e do not sell your data";

(b) Zoom maintains adequate security measures to safeguard and keep confidential users' personal information;

(c) Zoom limits its use of users' personal information "to determine the offers to make for [its] services, analyze trends on and run the marketing site, and understand users' movements around the marketing site"; and

(d) Zoom provides "[s]ecurity and encryption ... with complete end-to-end 256-bit AES encryption[.]"

154. In reliance on Zoom's representations, Plaintiffs and other Class members obtained Zoom accounts and provided Zoom with confidential, sensitive personal information.

155. Zoom's misrepresentations and omissions caused Plaintiffs and other Class members to become Zoom users and provide Zoom with their confidential, sensitive personal information. Plaintiffs and other Class members would not have done so, but for Zoom's misrepresentations and omissions.

156. Zoom's misrepresentations and omissions are unfair, unlawful, and fraudulent. Zoom's acts, as alleged above, are "unfair" because they offend an established public policy and are immoral, unethical, and unscrupulous or substantially injurious to consumers. Zoom's acts, as alleged above, are "unlawful" because they violate the common law and several California statutes, including the CCPA and CLRA. Zoom's acts, as alleged above, are "fraudulent" because they are likely to deceive the general public.

157. In addition to making these misrepresentations and omissions, Zoom also violated the UCL by (a) failing to timely notify Plaintiffs and other Class members of the unauthorized disclosure of, access to, and use of their personal information; (b) preventing Plaintiffs and other Class members from taking the necessary measures to remedy the unauthorized disclosure of their personal information; and (c) failing to maintain adequate security and proper encryption in Zoom's videoconferences.

158. Zoom's business practices violate the UCL also because Zoom (a) falsely represented that goods or services have characteristics they do not have, namely, adequate security; (b) falsely represented that its goods or services are of a particular standard when they are of another; (c) advertised its goods and services with intent not to sell them as advertised; (d) represented that the subject of a transaction was supplied in accordance with a previous representation when it was not; and (e) made material omissions regarding its safeguarding of users' personal information.

159. Plaintiffs and other Class members suffered injury in fact and lost money or property as the result of Zoom's violations of the UCL.

160. Plaintiffs request that Zoom be (a) enjoined from further violations of the UCL; and (b) required to restore to Plaintiffs and other Class members any money it had acquired by unfair competition, including restitution and restitutionary disgorgement.

Count VIII
Invasion of Privacy in
Violation of Common Law and the California Constitution

161. Plaintiffs repeat and incorporate by reference each and every allegation set forth above, as though fully set forth herein.

162. Under the common law and Section 1 in Article I of the California Constitution, Plaintiffs and the Class members have a reasonable expectation of privacy in their personal information, their electronic devices (including computers, tablets, and mobile phones), and their online behavior and history (including their use of Zoom's services).

163. The reasonableness of such expectations of privacy finds support in Zoom's

unique position to monitor Plaintiffs' and the Class members' behavior through its access to their electronic devices and videoconferences. The surreptitious, highly technical, and non-intuitive nature of Zoom's disclosure of their personal information further underscores the reasonableness of their expectations of privacy.

164. Plaintiffs' and Class members' privacy interest is legally protected because they have an interest in precluding the dissemination or misuse of sensitive information and an interest in making intimate personal decisions and conducting activities like videoconferencing without observation, intrusion, or interference.

165. Zoom shared Plaintiffs' and the Class members' personal information, without their authorization or consent, with third parties, including Facebook.

166. Zoom's acts and omissions caused the exposure and publicity of private details about Plaintiffs and other Class members — matters that are of no concern to the public.

167. This intrusion is highly offensive to a reasonable person. Zoom's conduct alleged above is particularly egregious because Zoom concealed its conduct from Plaintiffs and other Class members, and because Zoom represented to Plaintiffs and other Class members that it considered privacy to be "an extremely important topic" and took their privacy "very seriously."

168. As a direct and proximate result of Zoom's conduct, Plaintiffs and Class members were harmed by the public disclosure of their private affairs.

169. Plaintiffs and other Class members seek damages in an amount to be determined at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and on behalf of all members of the Class, respectfully request that the Court enter judgment in favor of them and against Zoom:

A. certifying this action as a class action under Federal Rule of Civil Procedure 23, appointing Plaintiffs as Class Representatives, and appointing their counsel as Class Counsel;

B. declaring that Zoom's conduct alleged in this complaint is unfair, unlawful, and fraudulent in violation of the CCPA, the CLRA, and the UCL, and that Zoom is liable for negligence, breach of implied contract, breach of the implied covenant of good faith and fair dealing, and unjust enrichment;

C. enjoining Zoom from engaging in the negligent, unfair, unlawful, and fraudulent business practices alleged in this complaint;

D. awarding Plaintiffs and other Class members actual, compensatory, consequential, punitive, and treble damages to the extent permitted by law, including statutory damages available under the CCPA;

E. ordering Zoom to disgorge all benefits and profits unjustly retained through its misconduct alleged in this complaint;

F. awarding Plaintiffs and other Class members pre-judgment and post-judgment interest;

G. awarding Plaintiffs and other Class members reasonable attorneys' fees and costs, including expert witness fees; and

H. granting such other and further relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury.

Dated: May 13, 2020

Respectfully submitted,

BOTTINI & BOTTINI, INC.
Francis A. Bottini, Jr. (SBN 175783)
Albert Y. Chang (SBN 296065)
Yury A. Kolesnikov (SBN 271173)

s/ Francis A. Bottini, Jr.
Francis A. Bottini, Jr.
7817 Ivanhoe Avenue, Suite 102
La Jolla, California 92037
Telephone: (858) 914-2001
Facsimile: (858) 914-2002
fbottini@bottinilaw.com
achang@bottinilaw.com
ykolesnikov@bottinilaw.com

COTCHETT, PITRE & MCCARTHY, LLP
Mark C. Molumphy (SBN 168009)
Tyson Redenbarger (SBN 294424)
Anya N. Thepot (SBN 318430)
San Francisco Airport Office Center
840 Malcolm Road, Suite 200
Burlingame, California 94010
Telephone: (650) 697-6000
Facsimile: (650) 697-0577
mmolumphy@cpmlegal.com
tredenbarger@cpmlegal.com
athepot@cpmlegal.com

Attorneys for Plaintiffs and the Class