

1 BOTTINI & BOTTINI, INC.
Francis A. Bottini, Jr. (SBN 175783)
2 fbottini@bottinilaw.com
3 Albert Y. Chang (SBN 296065)
achang@bottinilaw.com
4 Yury A. Kolesnikov (SBN 271173)
ykolesnikov@bottinilaw.com
5 7817 Ivanhoe Avenue, Suite 102
La Jolla, California 92037
6 Telephone: (858) 914-2001
7 Facsimile: (858) 914-2002

COTCHETT, PITRE & MCCARTHY, LLP
8 Mark C. Molumphy (SBN 168009)
mmolumphy@cpmlegal.com
9 Tyson Redenbarger (SBN 294424)
tredenbarger@cpmlegal.com
10 Anya N. Thepot (SBN 318430)
11 athepot@cpmlegal.com
San Francisco Airport Office Center
12 840 Malcolm Road, Suite 200
Burlingame, California 94010
13 Telephone: (650) 697-6000
14 Facsimile: (650) 697-0577

Attorneys for Plaintiffs and the Class

15
16 UNITED STATES DISTRICT COURT
17 NORTHERN DISTRICT OF CALIFORNIA
18 SAN JOSE DIVISION

19 SAINT PAULUS LUTHERAN CHURCH
and HEDDI N. CUNDLE, individually and
20 on behalf of themselves and all others
similarly situated,

21 Plaintiffs,

22 vs.

23 ZOOM VIDEO COMMUNICATIONS, INC.,

24 Defendant.
25
26
27
28

Case No. _____

Class Action

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

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

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

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

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

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

22 ¹ Coleen Shalby, *"Disturbing Zoom-Bombing" Incident Hits Fresno State Students,*
23 *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).

24 ² Valarie Honeycutt Spears, *Pornographic Video Appeared During "Zoom Bombing"*
25 *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).

26 ³ *FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-*
27 *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).

- 1 • failure to provide adequate security, as promised, to avoid breach and
- 2 infiltration (*e.g.*, “Zoombombing”) of users’ videoconferences; and
- 3 • unfair, unlawful, and deceptive business practices relating to Zoom’s data
- 4 security.

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

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

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

21 10. While Zoom enjoyed its success due to the hike of revenues and its stock price
22 resulting from the explosion of demands for its services, Zoom’s unlawful collection and use
23 of users’ personal information and its lack of adequate security came to light in a series of
24

25 ⁴ Zoom for Government, *available at* <https://zoom.us/government> (last visited Apr.
26 6, 2020) (featuring photos of law enforcement and military personnel at work and listing
27 under “Organizations that love Zoom” eight government agencies, including the CDC, DHS,
28 the Colorado Department of Corrections, the Hawaii State Department of Health, the Los
Angeles Police Department, and the City of San Jose).

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

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

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

14 13. Zoom's privacy violations and security breaches quickly commanded the
15 attention of 27 state attorneys general and the Federal Bureau of Investigation ("F.B.I."). On
16 March 30, 2020, the New York Attorney General sent a letter to Zoom expressing concerns
17 over and inquiring about its data-privacy and security practices. And on March 31, 2020, the
18

19 _____
20 ⁵ Joseph Cox, *Zoom iOS App Sends Data to Facebook Even If You Don't Have a*
21 *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](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").

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

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

28 ⁸ Aaron Tilley & Robert McMillan, *Zoom CEO: "I Really Messed Up" on Video*
29 *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*
30 *Misleading Marketing*, THE INTERCEPT, Mar. 31, 2020, available at [https://theintercept.
com/2020/03/31/zoom-meeting-encryption/](https://theintercept.com/2020/03/31/zoom-meeting-encryption/) (last visited May 11, 2020).

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

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

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

10 **PARTIES**

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

12 **A. Saint Paulus Lutheran Church**

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

19 17. In Saint Paulus’s long history, it survived the Great Earthquake and Fire of
20 1906, the social and cultural turmoil of the 1960s–70s, and a 1995 fire that destroyed its 103-
21 year-old cathedral building. Never did Saint Paulus imagine falling prey to Zoom’s deceptive
22 business practices and sex-offenders’ depraved hacking during this unprecedented COVID-
23 19 pandemic.

24 18. To conduct its weekly bible-studies class in compliance with the State’s stay-
25 at-home order, Ms. Cundle registered an account with Zoom on behalf of Saint Paulus using
26 an Apple computer on March 17, 2020. Beginning on March 23, 2020, Saint Paulus paid a
27 monthly fee for its Zoom account. Through Ms. Cundle and congregants, Saint Paulus has
28

1 used and accessed Zoom since March 25, 2020.

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

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

12 **B. Heddi N. Cundle**

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

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

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

25 24. In fact, Ms. Cundle registered with Zoom as a user and used Zoom's services
26 in reliance on Zoom's promises that (a) Zoom does not sell users' data; (b) Zoom takes
27 privacy seriously and adequately protects users' personal information; and (c) Zoom's
28

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

3 **II. Defendant Zoom Video Communications, Inc.**

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

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

13 **JURISDICTION AND VENUE**

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

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

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

24 **INTRADISTRICT ASSIGNMENT**

25 30. In compliance with Local Rule 3-2(b), Plaintiffs request that this action be
26 assigned to the San Jose Division of this District because a substantial part of the events or
27 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.

1 encryption to secure its videoconferences:

2 ***Meet securely***

3 ***End-to-end encryption for all meetings ...***

4 * * *

5 Protect your Meetings

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

- 7 • ***Secure a meeting with end-to-end encryption***

8 * * *

9 Enables HIPPA, PIPEDA & PHIPA Compliance

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

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

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

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

25 Client Application

26 Role-based user security

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

- 28 • ***Enable an end-to-end (E2E) encrypted meeting***

- 1 • Secure log-in using standard **username and password** ... sign-on
- 2 • Start **a secured meeting with password**
- 3 • Schedule a secured meeting with password

* * *

4 Meeting Security

5 Role-based user security

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

- 7 • **Secure a meeting with E2E encryption**

8 ...

- 9 • **Expel a participant or all participants**

- 10 • End a meeting

- 11 • **Lock a meeting**

12 ...

- 13 • Mute/unmute a participant or all participants

14 ...

- 15 • Enable/disable a participant or all participants to record ...

16 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.

17 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.

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

24 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

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

4 41. Likewise, Zoom’s stock price skyrocketed — trading at one point at a high of
5 \$164.94 per share (on March 23, 2020). Today, Zoom amasses over \$30 billion in market
6 capitalization. Zoom’s exponential growth of market capitalization is predicated upon users’
7 trust in its promises of data privacy and security. But these promises are false.

8 **II. Zoom Broke Its Promises of Data Privacy and Security**

9 **A. Zoom Collected and Disclosed Users’ Personal Information 10 Without Authorization or Consent**

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

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

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

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

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

9 Facebook told [*Vice*] it ***requires developers to be transparent***
10 ***with users about the data their apps send to Facebook.*** Facebook’s
11 terms say “If you use our pixels or SDK [(software development kits)], you
12 further represent and warrant that you have provided ***robust and***
13 ***sufficiently prominent notice to users regarding the Customer***
14 ***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.”

15 *See Vice Report.*

16 47. Indeed, after being confronted with *Vice*’s findings, “***Zoom confirmed the***
17 ***data collection*** in a statement to [*Vice*]”:

18 We originally implemented the ‘Login with Facebook’ feature using the
19 Facebook SDK in order to provide our users with another convenient way to
20 access our platform. However, ***we were recently made aware that the***
Facebook SDK was collecting unnecessary device data [as identified
by *Vice*.] ...

21 To address this, in the next few days, we will be removing the Facebook
22 SDK and reconfiguring the feature so that users will still be able to login with
23 Facebook via their browser. Users will need to update to the latest version of
24 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.

25 *See Vice Report.*

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

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

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

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

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

18 For Americans sheltering at home during the coronavirus pandemic,
19 the Zoom videoconferencing platform has become a lifeline, enabling millions
20 of people to easily keep in touch with family members, friends, students,
21 teachers and work colleagues.

22 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.

25 ***The undisclosed data mining adds to growing concerns***
about Zoom's business practices at a moment when public schools,
26 health providers, employers, fitness trainers, prime ministers and queer dance
27 parties are embracing the platform.

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

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

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

17 **B. Zoom Failed to Implement Adequate Security Protocols**
 18 **Jeopardizing Users’ Account Security**

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

22 An exploit for a zero-day remote code execution vulnerability affecting
 23 the Zoom Windows client is currently being sold for \$500,000, together with
 24 one designed to abused a bug in the video conferencing platform's macOS
 25 client.

26 * * *

27 As *BleepingComputer* reported on Monday, ***more than 500,000***
 28 ***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).

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

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

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

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

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

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

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

24 But when reached for comment about whether video meetings are
25 actually end-to-end encrypted, a Zoom spokesperson wrote, "**Currently, it**
26 **is not possible to enable E2E encryption for Zoom video meetings.**
Zoom video meetings use a combination of TCP and UDP. TCP connections
27 are made using TLS and UDP connections are encrypted with AES using a key
28 negotiated over a TLS connection."

1 The encryption that Zoom uses to protect meetings is TLS, the same
 2 technology that web servers use to secure HTTPS websites. This means that
 3 the connection between the Zoom app running on a user's computer or phone
 4 and Zoom's server is encrypted in the same way the connection between your
 5 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
 6 you have a Zoom meeting, the video and audio content will stay private from
 7 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.)

8 ...
 9 ***"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
 10 the Zoom cloud" through the networking between these machines.
 11

12 *See Intercept Report.*

13 60. According to one cryptographer, Professor Matthew D. Green of Johns
 14 Hopkins University's Department of Computer Science, Zoom is twisting the common
 15 meaning of "end-to-end" in a "***dishonest way***":
 16

17 "They're a little bit fuzzy about what's end-to-end encrypted," Green
 18 said of Zoom. "I think they're doing this in a slightly dishonest way. It would
 be nice if they just came clean."
 19

20 *See id.*

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

23 62. Zoom's dishonesty is particularly glaring in light of the fact that several of
 24 Zoom's competitors, including Apple FaceTime and Signal, offer real end-to-end encryption
 in their videoconferences:
 25

26 "If it's all end-to-end encrypted, you need to add some extra
 27 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,
 28

1 though, Green said, as demonstrated by Apple’s FaceTime, which allows group
2 video conferencing that’s end-to-end encrypted. “***It’s doable. It’s just not
3 easy.***”

3 *See Intercept Report.*

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

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

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

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

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

19 *See Post Report.*

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

22 An analysis by *The New York Times* found 153 Instagram accounts,
23 dozens of Twitter accounts and private chats, and several active message
24 boards on Reddit and 4Chan where thousands of people had gathered to
25 organize Zoom harassment campaigns, sharing meeting passwords and plans
26 for sowing chaos in public and private meetings. (Since this article’s
27 publication, Reddit has shut down the message boards where Zoom raids were
28 discussed.)

26 Zoom raiders often employ shocking imagery, racial epithets and
27 profanity to derail video conferences. Though a meeting organizer can remove
28 a participant at any time, the perpetrators of these attacks can be hard to

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

3 *See Times Zoombombing Report.*

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

8 69. In addition to the F.B.I., other state and federal authorities also intervened.
9 The attorneys generals of 27 states, including New York, have raised questions about privacy
10 issues and demanded that Zoom cooperate with them in multiple investigations. *See WSJ*
11 *Report*. Senator Richard Blumenthal of Connecticut wrote a letter to Zoom on March 31,
12 2020 demanding answers about Zoom’s “troubling history of software design practices and
13 security lapses.” *Id.* Senator Blumenthal expressed grave concerns over Zoom’s privacy
14 violations and security breaches:

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

18 *Id.* (internal quotation marks omitted).

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

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

28

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

3 **III. Plaintiffs’ Experience with Zoom and Zoombombing**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

16 **C. Zoom Rejected Saint Paulus’s Repeated Pleas to Improve Security**

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

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

25 90. In an email response dated May 6, 2020, Zoom’s Trust & Safety department
26 stated that it had identified the intruder and blocked the intruder “from joining future
27 meetings using the same Zoom software.” But Zoom refused to take any further action to
28

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

4 We identified in your meeting *a known serial offender who disrupts*
5 *open meetings by showing the same video*, and which *has been*
6 *reported multiple times to the authorities*. This intruder has the
following identifying information:

7 Christine (iPad)

8 The report ID for Christine (iPad) is 71731955. You can use this number when
9 you submit your report to link both reports.

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

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

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

20 **FRAUDULENT CONCEALMENT AND TOLLING**

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

26 **CLASS ACTION ALLEGATIONS**

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

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

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

1 Zoom's conduct;

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

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

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

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

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

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

27 102. **Superiority Under Rule 23(b)(3).** A class action is superior to other
28

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

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

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

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

19 CAUSES OF ACTION

20 Count I 21 Negligence

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

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

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

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

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

- 6 • disclosing Plaintiffs' and other Class members' personal information to
7 unauthorized third parties, including Facebook;
- 8 • allowing third parties to access the personal information of Plaintiffs and
9 other Class members;
- 10 • failing to implement and maintain adequate security measures to
11 safeguard users' personal information;
- 12 • failing to timely notify Plaintiffs and other Class members of the unlawful
13 disclosure of their personal information; and
- 14 • failing to maintain adequate security and proper encryption in Zoom's
15 videoconferences.

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

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

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

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

23 **Count II**
24 **Breach of Implied Contract**

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

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

1 which require the provision of confidential, sensitive personal information.

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

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

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

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

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

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

1 disclosure of their personal information; and

- 2 • failing to maintain adequate security and proper encryption in Zoom’s
3 videoconferences.

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

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

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

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

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

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

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

- 26 • disclosing Plaintiffs’ and other Class members’ personal information to
27 unauthorized third parties, including Facebook;
28 • allowing third parties to access the personal information of Plaintiffs and

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

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.

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

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

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

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

- 8 • disclosing Plaintiffs’ and other Class members’ personal information to
9 unauthorized third parties, including Facebook;
- 10 • allowing third parties to access the personal information of Plaintiffs and
11 other Class members;
- 12 • failing to implement and maintain adequate security measures to
13 safeguard users’ personal information;
- 14 • failing to, in a timely manner, (a) investigate the unauthorized disclosures
15 described above, and (b) notify Plaintiffs and other Class members of the
16 unauthorized disclosure of, access to, and use of their personal
17 information; and
- 18 • failing to maintain adequate security and proper encryption in Zoom’s
19 videoconferences.

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

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

28

- 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

1 forth above, as though fully set forth herein.

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

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

7 (a) “[w]e do not sell your data”;

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

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

13 (d) Zoom provides “[s]ecurity and encryption ... with complete end-to-end
14 256-bit AES encryption[.]”

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

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

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

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

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

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

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

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

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

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

22 **PRAYER FOR RELIEF**

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

25 A. certifying this action as a class action under Federal Rule of Civil Procedure
26 23, appointing Plaintiffs as Class Representatives, and appointing their counsel as Class
27 Counsel;

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

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

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

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

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

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

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

17 **DEMAND FOR JURY TRIAL**

18 Plaintiffs demand a trial by jury.

19 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)

22 s/ Francis A. Bottini, Jr.
23 _____
Francis A. Bottini, Jr.
24 7817 Ivanhoe Avenue, Suite 102
La Jolla, California 92037
25 Telephone: (858) 914-2001
Facsimile: (858) 914-2002
26 fbottini@bottinilaw.com
achang@bottinilaw.com
27 ykolesnikov@bottinilaw.com

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

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