POMERANTZ LLP
Jennifer Pafiti (SBN 282790)
1100 Glendon Avenue, 15th Floor
Los Angeles, California 90024
Telephone: (310) 405-7190
jpafiti@pomlaw.com

Attorney for Plaintiff

[Additional Counsel on Signature Page]

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

MICHAEL DRIEU, Individually and On Behalf of All Others Similarly Situated, Plaintiff, v. ZOOM VIDEO COMMUNICATIONS, INC., ERIC S. YUAN, and KELLY STECKELBERG, Defendants.	Case No. CLASS ACTION COMPLAINT FOR VIOLATIONS OF THE FEDERAL SECURITIES LAWS DEMAND FOR JURY TRIAL

Plaintiff Michael Drieu ("Plaintiff"), individually and on behalf of all other persons similarly situated, by Plaintiff's undersigned attorneys, for Plaintiff's complaint against Defendants, alleges the following based upon personal knowledge as to Plaintiff and Plaintiff's own acts, and information and belief as to all other matters, based upon, *inter alia*, the investigation conducted by and through Plaintiff's attorneys, which included, among other things, a review of the Defendants' public documents, conference calls and announcements made by Defendants, United States Securities and Exchange Commission ("SEC") filings, wire and press releases published by and regarding Zoom Video Communications, Inc. ("Zoom" or the "Company"), analysts' reports and advisories about the Company, and information readily obtainable on the Internet. Plaintiff believes that substantial evidentiary support will exist for the allegations set forth herein after a reasonable opportunity for discovery.

NATURE OF THE ACTION

1. This is a federal securities class action on behalf of a class consisting of all persons other than Defendants who purchased or otherwise acquired Zoom securities between April 18, 2019 and April 6, 2020, both dates inclusive (the "Class Period"), seeking to recover damages caused by Defendants' violations of the federal securities laws and to pursue remedies under Sections 10(b) and 20(a) of the Securities Exchange Act of 1934 (the "Exchange Act") and Rule 10b-5 promulgated thereunder, against the Company and certain of its top officials.

2. Zoom was founded in 2011 and is headquartered in San Jose, California. The Company was formerly known as Zoom Communications, Inc. and changed its name to Zoom Video Communications, Inc. in May 2012.

3. Zoom provides a video communications platform application ("app") that allows users to interact with each other primarily in the Americas, the Asia Pacific, Europe, the Middle East, and Africa. Users may connect through frictionless video, voice, chat, and content sharing.

The Company's cloud-native platform enables face-to-face video experiences and connects users across various devices and locations in a single meeting. The Company serves education, entertainment/media, enterprise infrastructure, finance, healthcare, manufacturing, non-profit/not for profit and social impact, retail/consumer products, and software/Internet industries, as well as individuals.

4. On March 22, 2019, Zoom filed a registration statement on Form S-1 with the SEC in connection with its initial public offering ("IPO"), which, after several amendments, was declared effective by the SEC on April 17, 2019 (the "Registration Statement").

5. On April 18, 2019, Zoom filed a prospectus on Form 424B4 with the SEC in connection with its IPO, which purported to provide information necessary for investors to consider before partaking in its IPO and purchasing the Company's newly publicly-issued stock (collectively with the Registration Statement, the "Offering Documents").

6. That same day, Zoom conducted its IPO and began trading publicly on the Nasdaq Global Select Market ("NASDAQ") under the ticker symbol "ZM." Pursuant to Zoom's IPO, the Company sold 9.91 million of the Company's shares to the public at the offering price of $36.00 per share.

7. Throughout the Class Period, Defendants made materially false and misleading statements regarding the Company's business, operational and compliance policies. Specifically, Defendants made false and/or misleading statements and/or failed to disclose that: (i) Zoom had inadequate data privacy and security measures; (ii) contrary to Zoom's assertions, the Company's video communications service was not end-to-end encrypted; (iii) as a result of all the foregoing, users of Zoom's communications services were at an increased risk of having their personal information accessed by unauthorized parties, including Facebook; (iv) usage of the Company's video communications services was foreseeably likely to decline when the foregoing facts came

to light; and (v) as a result, the Company's public statements were materially false and misleading at all relevant times.

8. The truth about the deficiencies in Zoom's software encryption began to come to light as early as July 2019. However, due in large part to the Company's obfuscation, it was not until the COVID-19 pandemic in March and April of 2020, with businesses and other organizations increasingly relying on Zoom's video communication software to facilitate remote work activity as governments increasingly implemented shelter-in-place orders, that the truth was more fully laid bare in a series of corrective disclosures. As it became clear through a series of news reports and admissions by the Company that Zoom had significantly overstated the degree to which its video communication software was encrypted, and organizations consequently prohibited its employees from utilizing Zoom for work activities, the Company's stock price plummeted, damaging investors.

9. As a result of Defendants' wrongful acts and omissions, and the precipitous decline in the market value of the Company's securities, Plaintiff and other Class members have suffered significant losses and damages.

JURISDICTION AND VENUE

10. The claims asserted herein arise under and pursuant to Sections 10(b) and 20(a) of the Exchange Act (15 U.S.C. §§ 78j(b) and 78t(a)) and Rule 10b-5 promulgated thereunder by the SEC (17 C.F.R. § 240.10b-5).

11. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1331 and Section 27 of the Exchange Act.

12. Venue is proper in this Judicial District pursuant to Section 27 of the Exchange Act (15 U.S.C. § 78aa) and 28 U.S.C. § 1391(b). Zoom is headquartered in this Judicial District,

Defendants conduct business in this Judicial District, and a significant portion of Defendants' activities took place within this Judicial District.

13. In connection with the acts alleged in this complaint, Defendants, directly or indirectly, used the means and instrumentalities of interstate commerce, including, but not limited to, the mails, interstate telephone communications, and the facilities of the national securities markets.

PARTIES

14. Plaintiff, as set forth in the attached Certification, acquired Zoom securities at artificially inflated prices during the Class Period and was damaged upon the revelation of the alleged corrective disclosures.

15. Defendant Zoom is a Delaware corporation with principal executive offices located at 55 Almaden Boulevard, 6th Floor, San Jose, California 95113. Zoom securities trade in an efficient market on the NASDAQ under the ticker symbol "ZM."

16. Defendant Eric S. Yuan ("Yuan") has served as Zoom's President and Chief Executive Officer at all relevant times.

17. Defendant Kelly Steckelberg ("Steckelberg") has served as Zoom's Chief Financial Officer at all relevant times.

18. Defendants Yuan and Steckelberg are sometimes referred to herein as the "Individual Defendants."

19. The Individual Defendants possessed the power and authority to control the contents of Zoom's SEC filings, press releases, and other market communications. The Individual Defendants were provided with copies of Zoom's SEC filings and press releases alleged herein to be misleading prior to or shortly after their issuance and had the ability and opportunity to prevent their issuance or to cause them to be corrected. Because of their positions with Zoom, and their

access to material information available to them but not to the public, the Individual Defendants knew that the adverse facts specified herein had not been disclosed to and were being concealed from the public, and that the positive representations being made were then materially false and misleading. The Individual Defendants are liable for the false statements and omissions pleaded herein.

20. Zoom and the Individual Defendants are sometimes collectively referred to herein as "Defendants."

SUBSTANTIVE ALLEGATIONS

Background

21. Zoom was founded in 2011 and is headquartered in San Jose, California. The Company was formerly known as Zoom Communications, Inc. and changed its name to Zoom Video Communications, Inc. in May 2012.

22. Zoom provides a video communications app that allows users to interact with each other primarily in the Americas, the Asia Pacific, Europe, the Middle East, and Africa. Users may connect through frictionless video, voice, chat, and content sharing. The Company's cloud-native platform enables face-to-face video experiences and connects users across various devices and locations in a single meeting. The Company serves education, entertainment/media, enterprise infrastructure, finance, healthcare, manufacturing, non-profit/not for profit and social impact, retail/consumer products, and software/Internet industries, as well as individuals.

23. On March 22, 2019, Zoom filed the Registration Statement on Form S-1 with the SEC in connection with its IPO, which, after several amendments, was declared effective by the SEC on April 17, 2019.

24. On April 18, 2019, Zoom filed a prospectus on Form 424B4 with the SEC in connection with its IPO, which purported to provide information necessary for investors to consider before partaking in its IPO and purchasing the Company's newly publicly-issued stock.

25. That same day, Zoom conducted its IPO and began trading publicly on the NASDAQ under the ticker symbol "ZM." Pursuant to Zoom's IPO, the Company sold 9.91 million of the Company's shares to the public at the offering price of $36.00 per share.

Materially False and Misleading Statements Issued During the Class Period

26. The Class Period begins on April 18, 2019, when Zoom conducted its IPO and its shares began publicly trading on the NASDAQ pursuant to the materially false or misleading statements or omissions contained in the Offering Documents. In the Offering Documents, Defendants touted that Zoom's "unique technology and infrastructure enable [*inter alia*] best-in-class reliability," and that Zoom "offer[s] robust security capabilities, ***including end-to-end encryption***, secure login, administrative controls and role-based access controls" (emphasis added).

27. Additionally, the Offering Documents touted that "[o]ne of the most important features of [Zoom's] platform is its broad interoperability with a range of diverse devices, operating systems and third-party applications"; that its "platform is accessible from the web and from devices running Windows, Mac OS, iOS, Android and Linux"; that the Company has "integrations with [*inter alia*] . . . a variety of other productivity, collaboration, data management and security vendors"; and that the Company "provide[s], develop[s] and create[s] applications for [its] platform partners that integrate[s] [its] platform with [its] partners' various offerings."

28. The Offering Documents also touted that, as part of Zoom's growth strategy, the Company "enable[s] developers to embed our platform into their own offerings through [*inter alia*]

. . . [its] cross-platform software development kits (SDKs),” such as those the Company used, or would eventually use, when linking users’ data to Facebook.

29. Additionally, the Offering Documents generally touted that Zoom’s “cloud-native platform delivers reliable, high-quality video that is easy to use, manage and deploy, provides an attractive return on investment, is scalable and easily integrates with physical spaces and applications”; that such “rich and reliable communications lead to interactions that build greater empathy and trust”; and that Defendants “strive to live up to the trust our customers place in us by delivering a communications solution that ‘just works.’”

30. The Offering Documents also assured investors that Zoom “strive[s] to comply with applicable laws, regulations, policies and other legal obligations relating to privacy, data protection and information security to the extent possible.”

31. Finally, the Offering Documents contained generic, boilerplate representations concerning Zoom’s risks related to cybersecurity, data privacy, and hacking, noting that the Company’s “security measures have on occasion, in the past, been, and may in the future be, compromised”; that “[c]onsequently, our products and services may be perceived as not being secure,” which “may result in customers and hosts curtailing or ceasing their use of our products, our incurring significant liabilities and our business being harmed”; and that “actual or perceived failure to comply with privacy, data protection and information security laws, regulations, and obligations could harm our business.” Plainly, the foregoing risk warnings were generic “catch-all” provisions that were not tailored to Zoom’s actual known risks concerning weaknesses in its cybersecurity and data protection systems.

32. On June 7, 2019, Zoom filed its first Quarterly Report on Form 10-Q with the SEC following its IPO, reporting the Company’s financial and operating results for the quarter ended April 30, 2019 (the “1Q20 10-Q”). The 1Q20 10-Q contained substantively the same statements

referenced in ¶¶ 27 and 29-31, *supra*, touting the way Zoom interacts with various operating systems and third-party applications, the trust its platform builds with customers and users, and the Company's efforts relating to privacy, data protection and information security; and providing generic "catch-all" provisions that were not tailored to Zoom's actual known risks concerning weaknesses in its cybersecurity and data protection systems.

33. Appended as an exhibit to the 1Q20 10-Q were signed certifications pursuant to the Sarbanes-Oxley Act of 2002 ("SOX"), wherein the Individual Defendants certified that the 1Q20 10-Q "fully complies with the requirements of Section 13(a) or 15(d) of the Securities Exchange Act of 1934 and that information contained in [the 1Q20 10-Q] fairly presents, in all material respects, the financial condition and results of operations of Zoom."

34. The statements referenced in ¶¶ 26-33 were materially false and misleading because Defendants made false and/or misleading statements, as well as failed to disclose material adverse facts about the Company's business, operational and compliance policies. Specifically, Defendants made false and/or misleading statements and/or failed to disclose that: (i) Zoom had inadequate data privacy and security measures; (ii) contrary to Zoom's assertions, the Company's video communications service was not end-to-end encrypted; (iii) as a result of all the foregoing, users of Zoom's communications services were at an increased risk of having their personal information accessed by unauthorized parties, including Facebook; (iv) usage of the Company's video communications services was foreseeably likely to decline when the foregoing facts came to light; and (v) as a result, the Company's public statements were materially false and misleading at all relevant times.

The Truth Begins to Emerge

35. On July 8, 2019, during intraday trading hours, security researcher Jonathan Leitschuh ("Leitschuh") linked an article published by him that day to his Twitter account, which

allegedly exposed a flaw allowing hackers to take over Zoom webcams. According to the article, "[a] vulnerability in the Mac Zoom Client allows any malicious website to enable your camera without your permission," and "[t]he flaw potentially exposes up to 750,000 companies around the world that use Zoom to conduct day-to-day business."

36. On this news, Zoom's stock price fell $1.12 per share, or 1.22%, to close at $90.76 per share on July 8, 2019.

37. Then, on July 11, 2019, public interest research center the Electronic Privacy Information Center ("EPIC") filed a complaint against Zoom before the U.S. Federal Trade Commission ("FTC"), alleging that the Company "placed at risk the privacy and security of the users of its services," that "Zoom intentionally designed their web conferencing service to bypass browser security settings and remotely enable a user's web camera without the consent of the user," and that, "[a]s a result, Zoom exposed users to the risk of remote surveillance, unwanted videocalls, and denial-of-service attacks." The complaint also alleged that "[w]hen informed of the vulnerabilities Zoom did not act until the risks were made public, several months after the matter was brought to the company's attention," that "Zoom exposed its users to a wide range of harms, many of which are ongoing," and that the Company's "business practices amount to unfair and deceptive practices under Section 5 of the FTC Act, subject to investigation and injunction by the [FTC]."

38. On this news, Zoom's stock fell $1.32 per share, or 1.42%, to close at $91.40 per share on July 11, 2019.

39. Following these disclosures, however, Zoom's stock price continued to trade at artificially inflated prices throughout the Class Period as a result of Defendants' continued misrepresentations and omissions concerning Zoom's data privacy and security mechanisms.

40. For example, on September 5, 2019, Zoom hosted an earnings call with investors and analysts to discuss the Company's second quarter financial results. In responding to a question regarding the Company's technology and architecture, Defendant Yuan stated, in relevant part:

> ***I think the combination of technology, ease-of-use, security will win the customer trust, right***. If you look at all other solutions out there today, all of them architecture is very old, right? Not a design for modern video cloud -- video first architecture. That's why we're ahead of any of our competitors for several years. Otherwise, I will go back to work all the weekend.

(Emphasis added.)

41. Then, on September 13, 2019, Zoom filed a Quarterly Report on Form 10-Q with the SEC, reporting the Company's financial and operating results for the quarter ended July 31, 2019 (the "2Q20 10-Q"). The 2Q20 10-Q contained substantively the same statements referenced in ¶¶ 27, 29-31, and 33, *supra*, touting the way Zoom interacts with various operating systems and third-party applications, the trust its platform builds with customers and users, and the Company's efforts relating to privacy, data protection and information security; providing generic "catch-all" provisions that were not tailored to Zoom's actual known risks concerning weaknesses in its cybersecurity and data protection systems; and containing SOX certifications signed by the Individual Defendants attesting to the accuracy and reliability of the financial report those certifications were appended to as an exhibit.

42. Additionally, in the 2Q20 10-Q's section dedicated to disclosing legal proceedings, Defendants asserted that "[w]e are not presently a party to any litigation the outcome of which, we believe, if determined adversely to us, would individually or taken together have a material adverse effect on our business, operating results, cash flows or financial condition," even despite the fact that legal proceedings had already been initiated by EPIC before the FTC on July 11, 2019, regarding Zoom's inadequate privacy and security measures, and at-risk software.

43. On December 9, 2019, Zoom filed another Quarterly Report on Form 10-Q with the SEC, reporting the Company's financial and operating results for the quarter ended October 31, 2019 (the "3Q20 10-Q"). The 3Q20 10-Q contained substantively the same statements referenced in ¶¶ 27, 29-31, 33, and 42, *supra*, touting the way Zoom interacts with various operating systems and third-party applications, the trust its platform builds with customers and users, the Company's efforts relating to privacy, data protection and information security, the lack of any legal proceedings likely to have a material adverse effect on the Company's business, operating results, cash flows or financial condition; providing generic "catch-all" provisions that were not tailored to Zoom's actual known risks concerning weaknesses in its cybersecurity and data protection systems; and containing SOX certifications signed by the Individual Defendants attesting to the accuracy and reliability of the financial report those certifications were appended to as an exhibit.

44. On March 4, 2020, Zoom hosted an earnings call with investors and analysts to discuss the Company's fourth quarter financial results. On that call, and while discussing an example of the security and compliance that Zoom's services ensured for its users, Defendant Yuan stated, in relevant part:

> I also want to thank VMware for trusting Zoom. VMware has been providing all employees, globally, access to Zoom meetings and digital workspace, and will soon utilize a large deployment of Zoom Phone. The easy, single sign-on access to Zoom from any device is enabled to leverage the VMware Workspace ONE platform, ***allowing employees to access all the applications they need from their device of choice while ensuring security and compliance***.

(Emphasis added.)

45. On March 20, 2020, six days before the truth fully emerged regarding Zoom's deficient security and privacy systems, Zoom filed its first Annual Report on Form 10-K with the SEC since its IPO, reporting the Company's financial and operating results for the quarter and year ended January 31, 2020 (the "2020 10-K"). As with the Offering Documents, the 2020 10-K

touted that Zoom's "unique technology and infrastructure enable [*inter alia*] best-in-class reliability."

46. The 2020 10-K also touted that the Company's Zoom Video Webinars feature "easily integrates with [*inter alia*] Facebook Live . . . providing access to large bases of viewers," without disclosing how integration with Facebook could implicate users' personal data, if at all.

47. Additionally, the 2020 10-K contained substantively the same statements referenced in ¶¶ 27-31, 33, and 42, *supra*, touting the way Zoom interacts with various operating systems and third-party applications, how the Company employed SDKs to partner with other digital platforms and app providers, the trust its platform builds with customers and users, the Company's efforts relating to privacy, data protection and information security, the lack of any legal proceedings likely to have a material adverse effect on the Company's business, operating results, cash flows or financial condition; providing generic "catch-all" provisions that were not tailored to Zoom's actual known risks concerning weaknesses in its cybersecurity and data protection systems; and containing SOX certifications signed by the Individual Defendants attesting to the accuracy and reliability of the financial report those certifications were appended to as an exhibit.

48. The statements referenced in ¶¶ 40-47 were materially false and misleading because Defendants made false and/or misleading statements, as well as failed to disclose material adverse facts about the Company's business, operational and compliance policies. Specifically, Defendants made false and/or misleading statements and/or failed to disclose that: (i) Zoom had inadequate data privacy and security measures; (ii) contrary to Zoom's assertions, the Company's video communications service was not end-to-end encrypted; (iii) as a result of all the foregoing, users of Zoom's communications services were at an increased risk of having their personal information accessed by unauthorized parties, including Facebook; (iv) usage of the Company's

video communications services was foreseeably likely to decline when the foregoing facts came to light; and (v) as a result, the Company's public statements were materially false and misleading at all relevant times.

The Truth Fully Emerges

49. On March 26, 2020—in the midst of the COVID-19 pandemic and shelter-in-place orders from multiple national and local governments, as businesses increasingly turned to Zoom's video communication software to facilitate remote work activity —*Motherboard*, Vice Media's technology news subsegment, reported that Zoom's "privacy policy do[es] [not] make clear . . . that the iOS version of the Zoom app is sending some analytics data to Facebook, even if Zoom users don't have a Facebook account," and that "Zoom is not forthcoming with the data collection or the transfer of it to Facebook." The article also alleged that "[t]he Zoom app notifies Facebook when the user opens the app, [and provides] details on the user's device such as the model, the time zone and city they are connecting from, which phone carrier they are using, and a unique advertiser identifier created by the user's device which companies can use to target a user with advertisements." The article also disclosed that "[s]everal days after Motherboard reached out for comment and a day after the publication of this piece, Zoom confirmed the data collection in a statement to Motherboard."

50. Then, on March 27, 2020, Zoom issued a statement by Defendant Yuan, disclosing "a change that [Defendants] have made regarding the use of Facebook's SDK" after being "made aware on Wednesday, March 25, 2020, that the Facebook SDK was collecting device information unnecessary for us to provide our services." Yuan admitted that "[t]he information collected by the Facebook SDK did not include information and activities related to meetings such as attendees, names, notes, etc., but rather included information about devices such as the mobile OS type and version, the device time zone, device OS, device model and carrier, screen size, processor cores,

and disk space," and that, "therefore [Defendants] decided to remove the Facebook SDK in [the] iOS client and have reconfigured the feature so that users will still be able to log in with Facebook via their browser." Yuan also promised that Defendants "remain firmly committed to the protection of our users' privacy," and that Defendants were "reviewing our process and protocols for implementing these features in the future to ensure this does not happen again."

51. The next trading day, on March 30, 2020, the *New York Times* reported that Zoom is under scrutiny by the office of New York State Attorney General ("AG"), Letitia James ("James"), "for its data privacy and security practices." According to the article, James's "office sent Zoom a letter asking what, if any, new security measures the company has put in place to handle increased traffic on its network and to detect hackers" in light of the recent COVID-19 pandemic. Specifically, the article, quoted James, who is "concerned that Zoom's existing security practices might not be sufficient to adapt to the recent and sudden surge in both the volume and sensitivity of data being passed through its network," and that, "[w]hile Zoom has remediated specific reported security vulnerabilities, [the office] would like to understand whether Zoom has undertaken a broader review of its security practices."

52. According to the *New York Times article*, James's investigation cited, *inter alia*, Leitschuh's earlier findings regarding webcam security issues with the Zoom app, the complaint that followed from EPIC, the recent revelations from Vice Media's *Motherboard* article, and the Company's reactive rather than proactive approach to addressing these issues. The article also noted other concerns cited by James's office, including how "the [Zoom] app may be circumventing state requirements protecting student data." According to the article, "some children's privacy experts and parents said they were particularly concerned about how children's personal details might be used," and "[s]ome districts have prohibited educators from using Zoom as a distance-learning platform." The article also stated that, "[o]ver the last few weeks, internet

trolls have exploited a Zoom screen-sharing feature to hijack meetings and do things like interrupt educational sessions or post white supremacist messages to a webinar on anti-Semitism—a phenomenon called 'Zoombombing.'"

53. That same day, *Bloomberg* reported that a user of Zoom's services had filed a lawsuit against the Company "who claims the popular video-conferencing service is illegally disclosing personal information." Specifically, the lawsuit alleged that Zoom "collects information when users install or open the Zoom application and shares it, without proper notice, to third parties including Facebook Inc.," that "Zoom's privacy policy doesn't explain to users that its app contains code that discloses information to Facebook and potentially other third parties," and that the Company's "wholly inadequate program design and security measures have resulted, and will continue to result, in unauthorized disclosure of its users' personal information."

54. Then, on March 31, 2020, the Federal Bureau of Investigation ("FBI") reportedly issued a warning about so-called "Zoom-bombing," the phenomenon identified by the *New York Times* where hackers can take over video-conferencing on the Company's app.

55. Additionally, that same day, multiple news sources, including *The Intercept* and *The Verge*, reported that Zoom's video conferencing software is not, in fact, end-to-end encrypted between meeting participants, contrary to the Company's assertions, and that Zoom was actually "using its own definition of the term, one that lets Zoom itself access unencrypted video and audio from meetings." Specifically, *The Intercept* article noted that, "despite this misleading marketing, the service actually does not support end-to-end encryption for video and audio content, at least as the term is commonly understood," and it "[i]nstead it offers what is usually called transport encryption," which is less secure. The article disclosed that after *The Intercept* reached out to Zoom for a comment about whether video meetings are actually end-to-end encrypted, a Zoom spokesperson wrote that, "[c]urrently, it is not possible to enable E2E [end-to-end] encryption for

Zoom video meetings," and that Zoom video meetings use the same encryption methods offered by web servers to secure certain websites. As noted by *The Intercept* article, 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."

56. Then, on April 1, 2020, during after-market hours, *Reuters* reported that Space Exploration Technologies Corp. ("SpaceX") had banned its employees from using Zoom's video conferencing software because of "significant privacy and security concerns," citing an internal memo reviewed by *Reuters* following the FBI's warning regarding "Zoombombing." According to *Reuters*, the National Aeronautics and Space Administration (NASA), one of SpaceX's largest customers, also decided to ban employee use of Zoom's app.

57. That same day, Defendant Yuan published a blog post entitled, "A Message to Our Users." In the post, Defendant Yuan admitted that "[the Company] recognize[s] that we have fallen short of the community's – and our own – privacy and security expectations."

58. Between March 27, 2020, and April 2, 2020, Zoom's stock price fell $29.77 per share, or 19.62%, to close at $121.93 per share on April 2, 2020.

59. On April 3, 2020, *The Street* reported that Defendant Yuan "recently dumped $38 million of the company's stock ahead of an investigation into security breaches at the video conferencing company," and that SEC "filings viewed by the Daily Mail showed that Yuan and several other senior executives sold millions of dollars worth of their shares while the company has been addressing privacy issues." Specifically, the article disclosed that Defendant "Yuan . . . made $10.5 million in sales on Jan[uary] 14, another $12.5 million on Feb[ruary] 12, and $15.5 million on March 16," while "Chief Marketing Officer Janine Pelosi has made close to $14 million in trades since February."

60. That same day, Connecticut AG William Tong ("Tong") announced his own office's investigation into Zoom's privacy and security practices. In a statement to *Politico*, Tong stated: "We are alarmed by the Zoom-bombing incidents and are seeking more information from the company about its privacy and security measures in coordination with other state attorneys general."

61. Also on April 3, 2020, Citizen Lab, an interdisciplinary laboratory based at the Munk School of Global Affairs & Public Policy at the University of Toronto, published a report "examin[ing] the encryption that protects meetings in the popular Zoom teleconference app." Citizen Lab found that Zoom has "rolled their own" (*i.e.*, built its own) encryption scheme, "which has significant weaknesses," and "identif[ied] potential areas of concern in Zoom's infrastructure, including observing the transmission of meeting encryption keys through China."

62. Later that day, during after-market hours, Zoom reportedly confirmed that, during its efforts to ramp up its server capacity to accommodate the massive influx of users over the past few weeks amid the COVID-19 pandemic, it "mistakenly" allowed two of its Chinese data centers to accept calls as a backup in the event of network congestion. According to Defendant Yuan, "[d]uring normal operations, Zoom clients attempt to connect to a series of primary datacenters in or near a user's region, and if those multiple connection attempts fail due to network congestion or other issues, clients will reach out to two secondary datacenters off of a list of several secondary datacenters as a potential backup bridge to the Zoom platform."

63. Then, over the weekend, on April 4, 2020, the *Wall Street Journal* reported that, in an interview with Defendant Yuan, Yuan had stated that "[i]f we mess up again, it's done," in discussing the mounting privacy issues Zoom was facing, and that "I really messed up as CEO" and "[t]his kind of thing shouldn't have happened."

64. On April 6, 2020, the following trading day, New York City's Department of Education announced that it had banned the use of Zoom in the city's classrooms, and the city's mayor, Bill de Blasio disclosed that there had "been an effort by the Department of Education to work with that company to ensure the privacy of our students to make sure their information could not be accessed wrongly," but that "[t]he chancellor and the team at the Department of Education do not believe the company has cooperated." Consequently, the city's Department of Education instead recommended Google or Microsoft Teams for classroom communications purposes amid the state's shelter-in-place order during the COVID-19 pandemic.

65. That same day, in a *Yahoo! Finance* article, it was reported that "[o]n April 1st, an actor in a popular dark web forum posted a link to a collection of 352 compromised Zoom accounts," according to a spokesperson for cybersecurity firm Sixgill; that, "[i]n comments on this post, several actors thanked him for the post, and one revealed intentions to troll the meetings"; that "these links included email addresses, passwords, meeting IDs, host keys and names, and the type of Zoom account"; that, according to Sixgill, "one belonged to a major U.S. healthcare provider, seven more to various educational institutions, and one to a small business"; that "[t]he accounts were listed for anyone to download, with the intent to troll and disrupt rather than profit"; and that, "given that many are using Zoom for business purposes, confidential information could be compromised."

66. Following these additional disclosures and news, Zoom's stock price fell $5.26 per share, or 4.10%, to close at $122.94 per share on April 6, 2020.

67. As a result of Defendants' wrongful acts and omissions, and the precipitous decline in the market value of the Company's securities, Plaintiff and other Class members have suffered significant losses and damages.

PLAINTIFF'S CLASS ACTION ALLEGATIONS

68. Plaintiff brings this action as a class action pursuant to Federal Rule of Civil Procedure 23(a) and (b)(3) on behalf of a Class, consisting of all those who purchased or otherwise acquired Zoom securities during the Class Period (the "Class"); and were damaged upon the revelation of the alleged corrective disclosures. Excluded from the Class are Defendants herein, the officers and directors of the Company, at all relevant times, members of their immediate families and their legal representatives, heirs, successors or assigns and any entity in which Defendants have or had a controlling interest.

69. The members of the Class are so numerous that joinder of all members is impracticable. Throughout the Class Period, Zoom securities were actively traded on the NASDAQ. While the exact number of Class members is unknown to Plaintiff at this time and can be ascertained only through appropriate discovery, Plaintiff believes that there are hundreds or thousands of members in the proposed Class. Record owners and other members of the Class may be identified from records maintained by Zoom or its transfer agent and may be notified of the pendency of this action by mail, using the form of notice similar to that customarily used in securities class actions.

70. Plaintiff's claims are typical of the claims of the members of the Class as all members of the Class are similarly affected by Defendants' wrongful conduct in violation of federal law that is complained of herein.

71. Plaintiff will fairly and adequately protect the interests of the members of the Class and has retained counsel competent and experienced in class and securities litigation. Plaintiff has no interests antagonistic to or in conflict with those of the Class.

72. Common questions of law and fact exist as to all members of the Class and predominate over any questions solely affecting individual members of the Class. Among the questions of law and fact common to the Class are:

- whether the federal securities laws were violated by Defendants' acts as alleged herein;
- whether statements made by Defendants to the investing public during the Class Period misrepresented material facts about the business, operations and management of Zoom;
- whether the Individual Defendants caused Zoom to issue false and misleading financial statements during the Class Period;
- whether Defendants acted knowingly or recklessly in issuing false and misleading financial statements;
- whether the prices of Zoom securities during the Class Period were artificially inflated because of the Defendants' conduct complained of herein; and
- whether the members of the Class have sustained damages and, if so, what is the proper measure of damages.

73. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. Furthermore, as the damages suffered by individual Class members may be relatively small, the expense and burden of individual litigation make it impossible for members of the Class to individually redress the wrongs done to them. There will be no difficulty in the management of this action as a class action.

74. Plaintiff will rely, in part, upon the presumption of reliance established by the fraud-on-the-market doctrine in that:

- Defendants made public misrepresentations or failed to disclose material facts during the Class Period;
- the omissions and misrepresentations were material;
- Zoom securities are traded in an efficient market;

- the Company's shares were liquid and traded with moderate to heavy volume during the Class Period;
- the Company traded on the NASDAQ and was covered by multiple analysts;
- the misrepresentations and omissions alleged would tend to induce a reasonable investor to misjudge the value of the Company's securities; and
- Plaintiff and members of the Class purchased, acquired and/or sold Zoom securities between the time the Defendants failed to disclose or misrepresented material facts and the time the true facts were disclosed, without knowledge of the omitted or misrepresented facts.

75. Based upon the foregoing, Plaintiff and the members of the Class are entitled to a presumption of reliance upon the integrity of the market.

76. Alternatively, Plaintiff and the members of the Class are entitled to the presumption of reliance established by the Supreme Court in *Affiliated Ute Citizens of the State of Utah v. United States*, 406 U.S. 128, 92 S. Ct. 2430 (1972), as Defendants omitted material information in their Class Period statements in violation of a duty to disclose such information, as detailed above.

COUNT I

(Violations of Section 10(b) of the Exchange Act and Rule 10b-5 Promulgated Thereunder Against All Defendants)

77. Plaintiff repeats and re-alleges each and every allegation contained above as if fully set forth herein.

78. This Count is asserted against Defendants and is based upon Section 10(b) of the Exchange Act, 15 U.S.C. § 78j(b), and Rule 10b-5 promulgated thereunder by the SEC.

79. During the Class Period, Defendants engaged in a plan, scheme, conspiracy and course of conduct, pursuant to which they knowingly or recklessly engaged in acts, transactions, practices and courses of business which operated as a fraud and deceit upon Plaintiff and the other members of the Class; made various untrue statements of material facts and omitted to state material facts necessary in order to make the statements made, in light of the circumstances under

which they were made, not misleading; and employed devices, schemes and artifices to defraud in connection with the purchase and sale of securities. Such scheme was intended to, and, throughout the Class Period, did: (i) deceive the investing public, including Plaintiff and other Class members, as alleged herein; (ii) artificially inflate and maintain the market price of Zoom securities; and (iii) cause Plaintiff and other members of the Class to purchase or otherwise acquire Zoom securities and options at artificially inflated prices. In furtherance of this unlawful scheme, plan and course of conduct, Defendants, and each of them, took the actions set forth herein.

80. Pursuant to the above plan, scheme, conspiracy and course of conduct, each of the Defendants participated directly or indirectly in the preparation and/or issuance of the quarterly and annual reports, SEC filings, press releases and other statements and documents described above, including statements made to securities analysts and the media that were designed to influence the market for Zoom securities. Such reports, filings, releases and statements were materially false and misleading in that they failed to disclose material adverse information and misrepresented the truth about Zoom's finances and business prospects.

81. By virtue of their positions at Zoom, Defendants had actual knowledge of the materially false and misleading statements and material omissions alleged herein and intended thereby to deceive Plaintiff and the other members of the Class, or, in the alternative, Defendants acted with reckless disregard for the truth in that they failed or refused to ascertain and disclose such facts as would reveal the materially false and misleading nature of the statements made, although such facts were readily available to Defendants. Said acts and omissions of Defendants were committed willfully or with reckless disregard for the truth. In addition, each Defendant knew or recklessly disregarded that material facts were being misrepresented or omitted as described above.

82. Information showing that Defendants acted knowingly or with reckless disregard for the truth is peculiarly within Defendants' knowledge and control. As the senior managers and/or directors of Zoom, the Individual Defendants had knowledge of the details of Zoom's internal affairs.

83. The Individual Defendants are liable both directly and indirectly for the wrongs complained of herein. Because of their positions of control and authority, the Individual Defendants were able to and did, directly or indirectly, control the content of the statements of Zoom. As officers and/or directors of a publicly-held company, the Individual Defendants had a duty to disseminate timely, accurate, and truthful information with respect to Zoom's businesses, operations, future financial condition and future prospects. As a result of the dissemination of the aforementioned false and misleading reports, releases and public statements, the market price of Zoom securities was artificially inflated throughout the Class Period. In ignorance of the adverse facts concerning Zoom's business and financial condition which were concealed by Defendants, Plaintiff and the other members of the Class purchased or otherwise acquired Zoom securities at artificially inflated prices and relied upon the price of the securities, the integrity of the market for the securities and/or upon statements disseminated by Defendants, and were damaged thereby.

84. During the Class Period, Zoom securities were traded on an active and efficient market. Plaintiff and the other members of the Class, relying on the materially false and misleading statements described herein, which the Defendants made, issued or caused to be disseminated, or relying upon the integrity of the market, purchased or otherwise acquired shares of Zoom securities at prices artificially inflated by Defendants' wrongful conduct. Had Plaintiff and the other members of the Class known the truth, they would not have purchased or otherwise acquired said securities, or would not have purchased or otherwise acquired them at the inflated prices that were paid. At the time of the purchases and/or acquisitions by Plaintiff and the Class, the true value of

Zoom securities was substantially lower than the prices paid by Plaintiff and the other members of the Class. The market price of Zoom securities declined sharply upon public disclosure of the facts alleged herein to the injury of Plaintiff and Class members.

85. By reason of the conduct alleged herein, Defendants knowingly or recklessly, directly or indirectly, have violated Section 10(b) of the Exchange Act and Rule 10b-5 promulgated thereunder.

86. As a direct and proximate result of Defendants' wrongful conduct, Plaintiff and the other members of the Class suffered damages in connection with their respective purchases, acquisitions and sales of the Company's securities during the Class Period, upon the disclosure that the Company had been disseminating misrepresented financial statements to the investing public.

COUNT II

(Violations of Section 20(a) of the Exchange Act Against The Individual Defendants)

87. Plaintiff repeats and re-alleges each and every allegation contained in the foregoing paragraphs as if fully set forth herein.

88. During the Class Period, the Individual Defendants participated in the operation and management of Zoom, and conducted and participated, directly and indirectly, in the conduct of Zoom's business affairs. Because of their senior positions, they knew the adverse non-public information about Zoom's misstatement of income and expenses and false financial statements.

89. As officers and/or directors of a publicly owned company, the Individual Defendants had a duty to disseminate accurate and truthful information with respect to Zoom's financial condition and results of operations, and to correct promptly any public statements issued by Zoom which had become materially false or misleading.

90. Because of their positions of control and authority as senior officers, the Individual Defendants were able to, and did, control the contents of the various reports, press releases and public filings which Zoom disseminated in the marketplace during the Class Period concerning Zoom's results of operations. Throughout the Class Period, the Individual Defendants exercised their power and authority to cause Zoom to engage in the wrongful acts complained of herein. The Individual Defendants therefore, were "controlling persons" of Zoom within the meaning of Section 20(a) of the Exchange Act. In this capacity, they participated in the unlawful conduct alleged which artificially inflated the market price of Zoom securities.

91. Each of the Individual Defendants, therefore, acted as a controlling person of Zoom. By reason of their senior management positions and/or being directors of Zoom, each of the Individual Defendants had the power to direct the actions of, and exercised the same to cause, Zoom to engage in the unlawful acts and conduct complained of herein. Each of the Individual Defendants exercised control over the general operations of Zoom and possessed the power to control the specific activities which comprise the primary violations about which Plaintiff and the other members of the Class complain.

92. By reason of the above conduct, the Individual Defendants are liable pursuant to Section 20(a) of the Exchange Act for the violations committed by Zoom.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff demands judgment against Defendants as follows:

A. Determining that the instant action may be maintained as a class action under Rule 23 of the Federal Rules of Civil Procedure, and certifying Plaintiff as the Class representative;

B. Requiring Defendants to pay damages sustained by Plaintiff and the Class by reason of the acts and transactions alleged herein;

C. Awarding Plaintiff and the other members of the Class prejudgment and post-judgment interest, as well as their reasonable attorneys' fees, expert fees and other costs; and

D. Awarding such other and further relief as this Court may deem just and proper.

DEMAND FOR TRIAL BY JURY

Plaintiff hereby demands a trial by jury.

Dated: April 7, 2020

Respectfully submitted,

POMERANTZ LLP

/s/ Jennifer Pafiti
Jennifer Pafiti (SBN 282790)
1100 Glendon Avenue, 15th Floor
Los Angeles, California 90024
Telephone: (310) 405-7190
E-mail: jpafiti@pomlaw.com

POMERANTZ LLP
Jeremy A. Lieberman
(*pro hac vice* application forthcoming)
J. Alexander Hood II
(*pro hac vice* application forthcoming)
600 Third Avenue, 20th Floor
New York, New York 10016
Telephone: (212) 661-1100
Facsimile: (212) 661-8665
Email: jalieberman@pomlaw.com
Email: ahood@pomlaw.com

POMERANTZ LLP
Patrick V. Dahlstrom
(*pro hac vice* application forthcoming)
10 South La Salle Street, Suite 3505
Chicago, Illinois 60603
Telephone: (312) 377-1181
Facsimile: (312) 377-1184
Email: pdahlstrom@pomlaw.com

BRONSTEIN, GEWIRTZ & GROSSMAN, LLC
Peretz Bronstein
(*pro hac vice* application forthcoming)

60 East 42nd Street, Suite 4600
New York, NY 10165
Telephone: (212) 697-6484
Facsimile: (212) 697-7296
Email: peretz@bgandg.com

Attorneys for Plaintiff