James M. Wagstaffe (#95535)
Frank Busch (#258288)
WAGSTAFFE, VON LOEWENFELDT, BUSCH & RADWICK LLP
100 Pine Street, Suite 725
San Francisco, California 94111
Telephone: (415) 357-8900
Facsimile: (415) 357-8910
wagstaffe@wvbrlaw.com
busch@wvbrlaw.com

Liaison Counsel for Plaintiff Kim Brams

[Additional counsel appear on signature page]

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

KIM BRAMS, Individually and on Behalf of All Others Similarly Situated, Plaintiff, vs. ZOOM VIDEO COMMUNICATIONS, INC., ERIC S. YUAN, and KELLY STECKELBERG, Defendants.	Case No. CLASS ACTION COMPLAINT FOR VIOLATION OF THE FEDERAL SECURITIES LAWS DEMAND FOR JURY TRIAL

INTRODUCTION

Plaintiff Kim Brams ("Plaintiff"), individually and on behalf of all others similarly situated, alleges the following based on personal knowledge as to Plaintiff and Plaintiff's own acts, and upon information and belief as to all other matters based upon the investigation conducted by and through Plaintiff's attorneys, which included, among other things, a review of press releases and other public statements issued by and regarding Zoom Video Communications, Inc. ("Zoom" or the "Company"), Zoom's filings with the U.S. Securities and Exchange Commission ("SEC"), and media and analyst reports about the Company. Plaintiff believes that substantial additional evidentiary support will exist for the allegations set forth herein after a reasonable opportunity for discovery.

SUMMARY OF THE ACTION

1. This is a securities class action on behalf of all persons other than Defendants (as defined herein) who purchased or otherwise acquired Zoom securities from April 18, 2019 through April 6, 2020, both dates inclusive (the "Class Period"), who were damaged thereby (the "Class"), seeking to pursue remedies under Sections 10(b) and 20(a) of the Securities Exchange Act of 1934 (the "Exchange Act"), and SEC Rule 10b-5 promulgated thereunder.

2. Zoom designs, develops, and sells a popular cloud-based communications platform that concentrates on video conferencing. Zoom's flagship product is "Zoom Meetings" which is a service that allows remote users to communicate with one another through video conferencing, collaborative meetings, text based chat and file sharing.

3. 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").

4. 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").

5. 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 approximately 9.91 million of the Company's shares to the public at the offering price of $36.00 per share.

6. 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.

7. 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 impact of 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.

8. As a result of Defendants' wrongful acts and misleading statements, 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

9. The claims asserted herein arise under 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.

10. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. §§ 1331 and 1337, and Section 27 of the Exchange Act, 15 U.S.C. § 78aa.

11. Venue is proper in this District pursuant to Section 27 of the Exchange Act, 15 U.S.C. § 78aa and 28 U.S.C. § 1391(b), as Zoom is headquartered in this District and many of the false and misleading statements alleged herein were disseminated from this District.

12. 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

13. Plaintiff purchased Zoom securities during the Class Period, as set forth in the certification attached hereto, and was damaged as the result of Defendants' wrongdoing as alleged in this complaint.

14. Defendant Zoom is a Delaware corporation and is headquartered in San Jose, California. The Company's stock is listed on the NASDAQ, an efficient market, under the ticker symbol "ZM." As of March 20, 2020, Zoom reported 127,468,829 outstanding shares of its Class A common stock.

15. Defendant Eric S. Yuan ("Yuan"), was at all relevant times, Zoom's founder, Chief Executive Officer ("CEO"), and President.

16. Defendant Kelly Steckelberg ("Steckelberg"), was at all relevant times, Zoom's Chief Financial Officer ("CFO").

17. Defendants Yuan and Steckelberg are sometimes referred to herein as the "Individual Defendants." Zoom and the Individual Defendants are collectively referred to herein as "Defendants."

18. The Individual Defendants, because of their positions with the Company, possessed the power and authority to control the contents of, *inter alia*, Zoom's quarterly reports, shareholder letters, press releases and presentations to securities analysts, money and portfolio managers and institutional investors, *i.e.*, the market. They were provided with copies of the Company's reports 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 cause them to be corrected. Because of their positions with the Company and their access to material non-public 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 and misleading statements pleaded herein.

SUBSTANTIVE ALLEGATIONS

Background

19. Zoom was founded in April 2011 by Defendant Yuan, and is headquartered in San Jose, California. The Company was originally known as Saasbee, Inc., and in February 2012 changed its name to Zoom Communications, Inc. The Company adopted its current name in May 2012. Zoom launched its first product, Zoom Meetings, in January 2013.

20. Zoom provides a video communications platform that allows users to 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.

21. Zoom Meetings is the cornerstone of the Company's platform, that ties all of Zoom's other products and features together. Zoom Meetings provide HD video, voice, chat and content sharing across mobile devices, desktops, laptops, telephones and conference room systems. The Company touts Zoom Meetings as a flexible tool for on-the-go employees who rely on their mobile device or tablet throughout their business day as we are the only service to have mobile start, join, scheduling and screen sharing.

22. Features of Zoom Meetings includes Zoom Chat, which allows users to send texts, images, audio files and content instantly across desktop, laptop, tablet and mobile devices, as well as Zoom Rooms, a software-based conference room system, which enables users to have frictionless Zoom Meetings in their physical meeting spaces.

23. Zoom generates revenues through a subscription based business model. While its most basic suite of products is offered free of charge, it offers Pro, Business, and Enterprise subscriptions, which offer enhanced features such as longer meeting times and increased meeting participants.

24. On March 22, 2019, Zoom began the process to engage in its IPO. On that date, Zoom filed the Registration Statement with the SEC. Zoom filed amendments to the Registration Statement on April 8, 2019 and April 16, 2019. The Registration Statement was declared effective by the SEC on April 17, 2019. On April 18, 2019 Zoom filed its prospectus on SEC Form 424B4, which together with the Registration Statement, form the Offering Materials.

25. Zoom completed its IPO on April 18, 2019. In connection with the IPO, the company sold 9,911,434 shares of its stock for the price of $36.00 per share. Additionally in the IPO, 10,958,131 shares of stock were also registered for resale by certain selling shareholders, including company insiders, investors, and affiliates. Finally the underwriters of Zoom's IPO were granted the option to purchase an additional 3,130,435 shares.

Materially False and Misleading Statements in Connection with the IPO

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."

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 "catchall" provisions that were not tailored to Zoom's actual known risks concerning weaknesses in its cybersecurity and data protection systems.

32. Additionally at the time of the IPO, Zoom had a published privacy policy which had been updated on March 19, 2019.[1] In the privacy policy, Zoom affirmed its commitment to protecting the data of its users, stating in pertinent part:

> Security of your Personal Data
>
> Zoom is committed to protecting the Personal Data you share with us. We utilize a combination of industry-standard security technologies, procedures, and organizational measures to help protect your Personal Data from unauthorized access, use or disclosure. When we transfer credit card information over the Internet, we protect it using Transport Layer Security (TLS) encryption technology.

False and Misleading Statements Following the IPO

33. Zoom updated its privacy policy on December 31, 2019.[2] The updated privacy policy contained substantively the same statements referenced in ¶ 32, *supra*.

[1] Privacy Policy, ZOOM (Mar. 19, 2019), http://web.archive.org/web/20200406014841/https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf (archived using Wayback Machine).

34. 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.

35. 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."

36. In or about June 2019, Zoom released a whitepaper detailing its security measures (the "Security Whitepaper").[3] In the Security Whitepaper, Zoom noted that the "***pre-meeting security capabilities are available to the meeting host***" included, *inter alia*, the ability to "***[e]nable an end-to-end (E2E) encrypted meeting***." Security Whitepaper, at 2. This was reiterated in the subsequent section entitled "Meeting Security." *Id*. at 3.

37. Additionally, as late as November 2019, Zoom's website noted that the meeting host could "***[s]ecure a meeting with end-to-end encryption***."[4] This statement remained live on Zoom's website throughout the Class Period.

38. The statements referenced in ¶¶ 26-37 were materially false and misleading because Defendants made false and/or misleading statements, as well as failed to disclose

[2] Privacy Policy, ZOOM (Dec. 31, 2019), https://web.archive.org/web/20200119034606/https://zoom.us/privacy (archived using Wayback machine).

[3] *See* SECURITY GUIDE (2019), http://web.archive.org/web/20200406014841/https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf (archived using Wayback Machine)

[4] *See Security at Zoom*, Zoom, https://web.archive.org/web/20191104094251/https://zoom.us/security (archived using Wayback Machine).

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 Is Partially Revealed

39. On July 8, 2019, during intraday trading hours, security researcher Jonathan Leitschuh ("Leitschuh") published an article which allegedly exposed a flaw allowing hackers to take over Zoom webcams.[5] 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."

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

41. 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"). The EPIC complaint alleged 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

[5] *See* Jonathan Leitschuh, *Zoom Zero Day: 4+ Million Webcams & maybe an RCE? Just get them to visit your website!*, MEDIUM (July 8, 2019), https://medium.com/bugbountywriteup/zoom-zero-day-4-million-webcams-maybe-an-rce-just-get-them-to-visit-your-website-ac75c83f4ef5.

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]."

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

43. 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.

44. 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.

45. 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 34, *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.

46. 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.

47. 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, 34, and 45, *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.

48. Zoom updated its privacy policy on February 23, 2020.[6] The updated privacy policy contained substantively the same statements referenced in ¶¶ 32 and 33, *supra*.

[6] Privacy Policy, ZOOM (Feb. 23, 2020), https://web.archive.org/web/20200314182734/https://zoom.us/privacy (archived using Wayback machine).

49. 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.

50. Zoom updated its privacy policy yet again on March 18, 2020.[7] The updated privacy policy contained substantively the same statements referenced in ¶¶ 32, 33, and 48, *supra*.

51. On March 20, 2020, 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."

52. 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.

53. Additionally, the 2020 10-K contained substantively the same statements referenced in ¶¶ 27-31, 34, and 45, *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

[7] Privacy Policy, ZOOM (Mar. 18, 2020), https://web.archive.org/web/20200325143843/https://zoom.us/privacy (archived using Wayback machine).

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.

54. The statements referenced in ¶¶ 44-53 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.

COVID-19 Causes Zoom's Usage Rates and Share Price to Skyrocket

55. Throughout the first quarter of 2020 and moving into April 2020, the COVID-19 pandemic placed millions of people under directives from their state and local governments to "stay at home" or "shelter in place." Accordingly, Zoom video meetings subsequently exploded in popularity because they provided a much needed communication service to the millions of people.

56. Because of Zoom's purported security, reliability, and ease of use the Company was seemingly well-positioned to capture this new market and see exponential growth. Therefore, while the majority of the markets were experiencing historic losses due to

the uncertainty surrounding COVID-19's impact on the global economy, Zoom shares soared. Specifically, while Zoom began 2020 with a share price of approximately $68.00 per share, it enjoyed meteoric gains thereafter, reaching Class Period highs of approximately $165.00 per share on March 23, 2020.

57. Zoom's exponentially increasing user base, however, would come with increased scrutiny into the Company's services. As revealed, *infra*, investors would soon learn that Zoom's long affirmed guarantees regarding privacy, security, and encryption, were anything but, thus revealing a lingering artificial inflation in the price of Zoom shares since the IPO. Further discussed, *infra*, Zoom insiders, including the Individual Defendants, cashed out when Zoom shares were at their apex, and directly on the cusp of these issues being revealed.

The Truth Is Fully Revealed Through Myriad Disclosures

58. On March 26, 2020, *Motherboard*, 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."[8] 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."

59. 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"

[8] Joseph Cox, *Zoom iOS App Sends Data to Facebook Even if You Don't Have a Facebook Account*, MOTHERBOARD (Mar. 26, 2020), https://www.vice.com/en_us/article/k7e599/zoom-ios-app-sends-data-to-facebook-even-if-you-dont-have-a-facebook-account.

after being "made aware on Wednesday, March 25, 2020, that the Facebook SDK was collecting device information unnecessary for us to provide our services."[9] 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."

60. On March 29, 2020 Zoom updated its privacy policy to be more transparent in light of the recent public scrutiny.[10]

61. The next trading day, on March 30, 2020, the *New York Times* reported that Zoom was under scrutiny by the office of New York State Attorney General ("AG"), Letitia James ("James"), "for its data privacy and security practices."[11] 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."

---

[9] Eric S. Yuan, *Zoom's Use of Facebook's SDK in iOS Client*, ZOOM (Mar. 27, 2020), https://blog.zoom.us/wordpress/2020/03/27/zoom-use-of-facebook-sdk-in-ios-client/.

[10] *See Privacy Policy*, ZOOM, https://zoom.us/privacy.

[11] Danny Hakim and Natasha Singer, *New York Attorney General Looks Into Zoom's Privacy Practices*, N.Y. TIMES (Mar. 30, 2020), https://www.nytimes.com/2020/03/30/technology/new-york-attorney-general-zoom-privacy.html.

62. 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.'"

63. 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."[12] 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."

[12] Joel Rosenblatt, *Zoom Sued for Allegedly Illegally Disclosing Private Data*, BLOOMBERG (Mar. 30, 2020), https://www.bloomberg.com/news/articles/2020-03-31/zoom-sued-for-allegedly-illegally-disclosing-personal-data.

64. Finally on March 30, 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.[13]

65. Additionally, that same day *The Intercept* 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."[14] 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.

66. The article by *The Intercept* also disclosed that after the publication had 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."

67. On March 31, 2020, the second consumer class action was filed against the Company, captioned *Taylor v. Zoom Video Communications, Inc.*, No. 20-cv-0217 (N.D. Cal.).

68. On April 1, 2020, *Reuters* reported that Space Exploration Technologies Corp. ("SpaceX") had banned its employees from using Zoom's video conferencing software

[13] Kristen Setera, *FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic*, FBI (Mar. 30, 2020), https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic.

[14] Micah Lee and Yael Grauer, *Zoom Meetings Aren't End-to-End Encrypted, Despite Misleading Marketing*, THE INTERCEPT (Mar. 31, 2020), https://theintercept.com/2020/03/31/zoom-meeting-encryption/.

because of "significant privacy and security concerns," citing an internal memo reviewed by *Reuters* following the FBI's warning regarding "Zoombombing."[15] 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.

69. Additionally on April 1, 2020, a blog reported that "Patrick Wardle, a macOS security researcher and former hacker for the National Security Agency, has uncovered two new local security vulnerabilities in the latest version of the Mac Zoom client."[16] The first noted flaw was related to Zoom's installation process "which is done without user interaction." Based on this process, "a user or piece of malware with low-level privileges can gain root access to a computer — the highest level of privilege." The second, more troubling flaw, according to the expose, "allows a local user or piece of malware to piggyback on Zoom's camera and microphone permissions." By virtue of this vulnerability, "[a]n attacker [could] inject malicious code into Zoom's process space and 'inherit' camera and microphone permissions, allowing them to hijack them without a user's knowledge."

70. In what would be a troubling day for the Company, *Motherboard* published another article detailing that a security flaw in Zoom's products was leaking users' email addresses and photos to strangers.[17] The issue, according to the *Motherboard* article, was due to "Zoom's 'Company Directory' setting, which automatically adds other people to a user's lists of contacts if they signed up with an email address that shares the same domain." In practice, however, Zoom users who signed up with personal email addresses were "pooled . . .

---

[15] Munsif Vengattil and Joey Roulette, *Elon Musk's SpaceX bans Zoom over privacy concerns –memo*, REUTERS (Apr. 1, 2020), https://www.reuters.com/article/us-spacex-zoom-video-commn/elon-musks-spacex-bans-zoom-over-privacy-concerns-memo-idUSKBN21J71H.

[16] Mike Peterson, *Two more macOS Zoom flaws surface, as lawsuit & government probe loom*, APPLE INSIDER (Apr. 1, 2020), https://appleinsider.com/articles/20/04/01/two-more-macos-zoom-flaws-surface-as-lawsuit-government-probe-loom.

[17] Joseph Cox, *Zoom is Leaking Peoples' Email Addresses and Photos to Strangers*, MOTHERBOARD (Apr. 1, 2020), https://www.vice.com/en_us/article/k7e95m/zoom-leaking-email-addresses-photos.

together with thousands of other people as if they all worked for the same company, exposing their personal information to one another."

71. That same day, Defendant Yuan published a blog post entitled, "A Message to Our Users."[18] In the post, which was in response to mounting public outcry, Defendant Yuan admitted that "[the Company] recognize[s] that we have fallen short of the community's – and our own – privacy and security expectations."

72. On April 2, 2020, security expert Brian Krebs revealed that an automated tool had been created to the purpose of finding Zoom meetings to engage in online vandalism.[19] According to the article, because all Zoom meeting IDs consist of nine to eleven digits, hackers "figured out they can simply guess or automate the guessing of random IDs within that space of digits." To assist in the process, hackers had apparently constructed an automated tool known as "zWarDial" to seek out Zoom meetings to disrupt. Zoom responded to questions by stating that moving forward all meetings would be password protected by default.

73. Additionally on April 2, 2020, *The Verge* published an article also discussing zWarDial.[20] The article noted that "[i]n addition to being able to find around 100 meetings per hour, one instance of zWarDial can successfully determine a legitimate meeting ID 14 percent of the time."

74. Finally on April 2, 2020, *The New York Times* reported that "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

[18] Eric S. Yuan, *A Message to Our Users*, ZOOM (Apr. 1, 2020) https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/.

[19] Brian Krebs, *'War Dialing' Tool Exposes Zoom's Password Problems*, KREBS ON SECURITY (Apr. 2, 2020), https://krebsonsecurity.com/2020/04/war-dialing-tool-exposes-zooms-password-problems/.

[20] Jay Peters, *Automated tool can find 100 Zoom meeting IDs per hour*, THE VERGE (Apr. 2, 2020), https://www.theverge.com/2020/4/2/21206061/zoom-meeting-id-zwardial-automated-tool.

even notifying them that someone else was snooping on them."[21] According to the article, "[t]he undisclosed data mining adds to growing concerns about Zoom's business practices at a moment when public schools, health providers, employers, fitness trainers, prime ministers and queer dance parties are embracing the platform."

75. In light of the storm of bad publicity concerns about the many vulnerabilities in the Zoom platform, the Company's share price experience significant declines. Specifically, between March 27, 2020, and April 2, 2020, Zoom's stock price fell $29.77 per share, or 19.62 percent, to close at $121.93 per share on April 2, 2020.

76. On April 3, 2020, *The Washington Post* reported that "[t]housands of personal Zoom videos have been left viewable on the open Web, highlighting the privacy risks to millions of Americans as they shift many of their personal interactions to video calls in an age of social distancing."[22] According to the article, "[v]ideos viewed by The Washington Post included one-on-one therapy sessions; a training orientation for workers doing telehealth calls that included people's names and phone numbers; small-business meetings that included private company financial statements; and elementary school classes, in which children's faces, voices and personal details were exposed." The article noted that "[m]any of the videos appear[ed] to have been recorded through Zoom's software and saved onto separate online storage space without a password." The article attributed the shocking oversight to the fact that "Zoom names every video recording in an identical way, a simple online search can reveal a long stream of videos elsewhere that anyone can download and watch."

77. 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

---

[21] Aaron Krolik and Natasha Singer, *A Feature on Zoom Secretly Displayed Data From People's LinkedIn Profiles*, N.Y. TIMES (Apr. 2, 2020), https://www.nytimes.com/2020/04/02/technology/zoom-linkedin-data.html.

[22] Drew Harwell, *Thousands of Zoom video calls left exposed on open Web*, WASH. POST (Apr. 3, 2020), https://www.washingtonpost.com/technology/2020/04/03/thousands-zoom-video-calls-left-exposed-open-web/.

app."[23] 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."

78. 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.[24] 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."

79. Additionally on April 3, 2020, Democratic Rep. Jerry McNerney of California and eighteen of his Democratic colleagues from the House Committee on Energy and Commerce sent a letter to Yuan raising concerns and questions regarding the company's privacy practices. The letter requested a response from Zoom by April 10.[25]

80. On April 3, 2020, a third consumer class action was filed against the Company, captioned Ohlweiler v. Zoom Video Communications, Inc., No. 20-cv-03165 (C.D. Cal.).

81. 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

---

[23] *Move Fast and Roll Your Own Crypto: A Quick Look at the Confidentiality of Zoom Meetings*, CITIZEN LAB (Apr. 3, 2020), https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/.

[24] Eric S. Yuan, *Response to Research From University of Toronto's Citizen Lab*, ZOOM (Apr. 3, 2020), https://blog.zoom.us/wordpress/2020/04/03/response-to-research-from-university-of-torontos-citizen-lab/.

[25] *Available at* https://mcnerney.house.gov/sites/mcnerney.house.gov/files/Letter%20to%20Zoom_04.03.2020.pdf.

mounting privacy issues Zoom was facing, and that "I really messed up as CEO" and "[t]his kind of thing shouldn't have happened."[26]

82. On April 6, 2020, the following trading day, multiple news sources, including the *New York Post*, reported that New York City's Department of Education announced ("DOE") that it had banned the use of Zoom in the city's classrooms, and the city's mayor, Bill de Blasio disclosed that "there's been an effort" by DOE officials to work with Zoom in order to "ensure the privacy of our students to make sure their information could not be accessed wrongly" and officials "do not believe the company has cooperated."[27] 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.

83. 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."[28]

---

[26] Aaron Tilley and Robert McMillan, *Zoom CEO: 'I Really Messed Up' on Security as Coronavirus Drove Video Tool's Appeal*, W.S.J. (Apr. 4, 2020), https://www.wsj.com/articles/zoom-ceo-i-really-messed-up-on-security-as-coronavirus-drove-video-tools-appeal-11586031129.

[27] Natalie Musumeci, *DOE bans schools using Zoom for remote learning amid security concerns*, N.Y. POST (Apr. 6, 2020), https://nypost.com/2020/04/06/doe-pulls-plug-on-schools-using-zoom-amid-security-concerns/.

[28] Ethan Wolff-Mann, *Hackers are posting verified Zoom accounts on the dark web*, YAHOO! FINANCE (Apr. 6, 2020), https://nz.finance.yahoo.com/news/hackers-are-posting-verified-zoom-accounts-on-the-dark-web-161442319.html.

84. 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.

85. 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.

Zoom Executives Engage in Substantial and Suspicious Insider Trading

86. Directly prior to the precipitous declines in the value of Zoom stock, Company executives, including Defendant Yuan, sold off substantial portions of their personally held Zoom shares. These sales were made while Company shares were trading at historic highs, bolstered even further by the artificial inflation which had lingered hidden in the price of Zoom shares since its inception as a publicly traded company. These suspiciously timed and unusual sales represented a windfall for Zoom insiders, including Pelosi Janine, Zoom's Chief Marketing Officer ("CMO"), who sold off over $30 million worth of Company shares on March 30, 2020 alone, and are therefore indicative of Defendants' fraud discussed herein. These trades are as follows:

Filer Name	Transaction Date	Average Sale Price	Shares Sold	Total Proceeds
Defendant Yuan	03.16.2020 03.17.2020	$112.18 $108.20	70,143 70,143	$7,949,838.34 $7,583,527.32
TOTAL:			**140,286**	**$15,533,365.66**
Defendant Steckelberg	03.23.2020	$126.17	11,067	$1,400,901.32
Pelosi Janine (Chief Marketing Officer)	03.09.2020 03.16.2020 03.30.2020	$109.08 $108.33 $157.76	31,850 15,623 190,930	$3,437,254.28 $1,689,128.78 $30,180,944.44
TOTAL:			**238,403**	**$35,307,327.50**
Subotovsky Santiago (Director)	03.10.2020 03.19.2020	$108.97 $121.13	73,168 73,168	$7,948,598.53 $8,851,521.37
TOTAL:			**146,336**	**$16,800,119.90**

UNDISCLOSED ADVERSE FACTS

87. At all relevant times, the market for Zoom securities was open, well-developed and efficient. As a result of Defendants' false statements and manipulative conduct, Zoom securities traded at artificially inflated prices during the Class Period. Plaintiff and other members of the Class purchased or otherwise acquired the Company's securities relying upon the integrity of the market price of the Company's securities and market information relating to Zoom, and have been damaged thereby.

88. During the Class Period, Defendants materially misled the investing public, thereby purposely inflating the price of Zoom's securities, by publicly issuing false and/or misleading statements and/or omitting to disclose material facts necessary to make Defendants' statements, as set forth herein, not false and/or misleading. These statements and omissions were materially false and/or misleading in that they failed to disclose material adverse information and/or misrepresented the truth about Zoom's business, operations, and prospects as alleged herein.

89. At all relevant times, the material misrepresentations and omissions particularized in this Complaint directly or proximately caused, or were a substantial contributing cause, of the damages sustained by Plaintiff and other members of the Class. As described herein, during the Class Period, Defendants made, or caused to be made, a series of materially false and/or misleading statements about Zoom's financial well-being and prospects. These material misstatements and/or omissions had the cause and effect of creating in the market an unrealistically positive assessment of the Company and its financial well-being and prospects, thus causing the Company's securities to be overvalued and artificially inflated at all relevant times. Defendants' materially false and/or misleading statements during the Class Period resulted in Plaintiff and other members of the Class transacting in the Company's securities at artificially inflated prices, thus causing the damages complained of herein.

ADDITIONAL SCIENTER ALLEGATIONS

90. During the Class Period, as alleged herein, the Defendants acted with scienter in that the Defendants knew or were reckless as to whether the public documents and statements issued or disseminated in the name of the Company during the Class Period were materially false and misleading; knew or were reckless as to whether such statements or documents would be issued or disseminated to the investing public; and knowingly and substantially participated or acquiesced in the issuance or dissemination of such statements or documents as primary violations of the federal securities laws.

91. The Defendants permitted Zoom to release these false and misleading statements and failed to file the necessary corrective disclosures, which artificially inflated the value of the Company's securities.

92. As set forth herein, the Defendants, by virtue of their receipt of information reflecting the true facts regarding Zoom, their control over, receipt, and/or modification of Zoom's allegedly materially misleading statements and omissions, and/or their positions with the Company that made them privy to confidential information concerning Zoom, participated in the fraudulent scheme alleged herein.

93. The Defendants are liable as participants in a fraudulent scheme and course of conduct that operated as a fraud or deceit on those who purchased or otherwise acquired Zoom securities by disseminating materially false and misleading statements and/or concealing material adverse facts. The scheme deceived the investing public regarding Zoom's business, operations, and management and the intrinsic value of Zoom common stock and caused Plaintiff and members of the Class to transact in Zoom securities at artificially inflated prices.

LOSS CAUSATION/ECONOMIC LOSS

94. During the Class Period, as detailed herein, Defendants made false and misleading statements and engaged in a scheme to deceive the market and a course of conduct that artificially inflated the prices of Zoom securities, and operated as a fraud or deceit on

Class Period purchasers of Zoom securities by misrepresenting the Company's business and prospects. Later, when Defendants' prior misrepresentations and fraudulent conduct became known to the market, the price of Zoom securities declined as the prior artificial inflation came out of the price over time. As a result of their purchases of Zoom securities during the Class Period, Plaintiff and other members of the Class suffered economic loss, *i.e.*, damages, under the federal securities laws.

APPLICABILITY OF PRESUMPTION OF RELIANCE: FRAUD ON THE MARKET

95. Plaintiff will rely upon the presumption of reliance established by the fraud-on-the-market doctrine in that, among other things:

(a) Defendants made public misrepresentations or failed to disclose material facts during the Class Period;

(b) the omissions and misrepresentations were material;

(c) the Company's securities traded in an efficient market;

(d) the misrepresentations alleged would tend to induce a reasonable investor to misjudge the value of the Company's securities; and

(e) Plaintiff and other members of the Class purchased or otherwise acquired Zoom securities between the time Defendants misrepresented or failed to disclose material facts and the time the true facts were disclosed, without knowledge of the misrepresented or omitted facts.

96. At all relevant times, the markets for Zoom securities were efficient for the following reasons, among others:

(a) as a regulated issuer, Zoom filed periodic public reports with the SEC;

(b) Zoom regularly communicated with public investors via established market communication mechanisms, including through regular disseminations of press releases on the major news wire services and through other wide-ranging public disclosures, such as communications with the financial press, securities analysts, and other similar reporting services;

(c) Zoom was followed by several securities analysts employed by major brokerage firm(s) who wrote reports that were distributed to the sales force and certain customers of their respective brokerage firm(s) and that were publicly available and entered the public marketplace; and

(d) Zoom securities were actively traded in an efficient market, namely the NASDAQ, under the ticker symbol "ZM."

97. As a result of the foregoing, the market for Zoom securities promptly digested current information regarding Zoom from publicly available sources and reflected such information in Zoom's stock price. Under these circumstances, all those who purchased or otherwise acquired Zoom securities during the Class Period suffered similar injury through their purchase of Zoom securities at artificially inflated prices and the presumption of reliance applies.

98. Further, to the extent that the Defendants concealed or improperly failed to disclose material facts with regard to the Company, Plaintiff is entitled to a presumption of reliance in accordance with *Affiliated Ute Citizens of Utah v. United States*, 406 U.S. 128, 153 (1972).

NO SAFE HARBOR

99. The statutory safe harbor provided for forward-looking statements under certain circumstances does not apply to any of the allegedly false statements pleaded in this Complaint. The statements alleged to be false and misleading herein all relate to then-existing facts and conditions. In addition, to the extent certain of the statements alleged to be false may be characterized as forward looking, they were not identified as "forward-looking statements" when made and there were no meaningful cautionary statements identifying important factors that could cause actual results to differ materially from those in the purportedly forward-looking statements. In the alternative, to the extent that the statutory safe harbor is determined to apply to any forward-looking statements pleaded herein, Defendants are liable for those false forward-looking statements because at the time each of those

forward-looking statements were made, the speaker had actual knowledge that the forward-looking statement was materially false or misleading, and/or the forward-looking statement was authorized or approved by an executive officer of Zoom who knew that the statement was false when made.

CLASS ACTION ALLEGATIONS

100. Plaintiff brings this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of all persons who purchased or otherwise acquired Zoom securities from April 18, 2019 through April 6, 2020, both dates inclusive. Excluded from the Class are: Defendants; the officers and directors of the Company during the Class Period (the "Excluded D&Os"); members of Defendants' and the Excluded D&Os' immediate families; the subsidiaries and affiliates of the Company, including the Company's employee retirement and benefit plan(s) and their participants or beneficiaries, to the extent they made purchases through such plan(s); and any entity in which Defendants or the Excluded D&Os have or had a controlling interest; and the legal representatives, heirs, successors or assigns of any excluded person or entity.

101. The members of the Class are so numerous that joinder of all members is impracticable. The disposition of their claims in a class action will provide substantial benefits to the parties and the Court. As of March 20, 2020, Zoom reported 127,468,829 outstanding shares of its Class A common stock.

102. There is a well-defined community of interest in the questions of law and fact involved in this case. Questions of law and fact common to the members of the Class which predominate over questions which may affect individual Class members include:

(a) Whether the Exchange Act was violated by Defendants;

(b) Whether Defendants omitted and/or misrepresented material facts;

(c) Whether Defendants' statements omitted material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading;

(d) Whether Defendants knew or recklessly disregarded that their statements were false and misleading;

(e) Whether the price of Zoom securities was artificially inflated; and

(f) The extent of damage sustained by Class members and the appropriate measure of damages.

103. Plaintiff's claims are typical of those of the Class because Plaintiff and the Class sustained damages from Defendants' wrongful conduct.

104. Plaintiff will adequately protect the interests of the Class and has retained counsel experienced in securities class action litigation. Plaintiff has no interests that conflict with those of the Class.

105. A class action is superior to other available methods for the fair and efficient adjudication of this controversy.

CLAIMS FOR RELIEF

COUNT I
For Violation of Section 10(b) of the Exchange Act and Rule 10b-5 Against All Defendants

106. Plaintiff repeats and realleges each and every allegation contained in the foregoing paragraphs as if fully set forth herein.

107. During the Class Period, Defendants disseminated or approved the false statements specified above, which they knew or recklessly disregarded were misleading in that they contained misrepresentations and failed to disclose material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading.

108. Defendants violated Section 10(b) of the Exchange Act and Rule 10b-5 in that they:

(a) Employed devices, schemes, and artifices to defraud;

(b) Made untrue statements of material facts or 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; or

(c) Engaged in acts, practices, and a course of business that operated as a fraud or deceit upon plaintiff and others similarly situated in connection with their purchases of Zoom securities during the Class Period.

109. Plaintiff and the Class have suffered damages in that, in reliance on the integrity of the market, they paid artificially inflated prices for Zoom securities. Plaintiff and the Class would not have purchased Zoom securities at the prices they paid, or at all, if they had been aware that the market prices had been artificially and falsely inflated by Defendants' misleading statements.

110. As a direct and proximate result of these Defendants' wrongful conduct, Plaintiff and the other members of the Class suffered damages in connection with their purchases of Zoom securities during the Class Period.

COUNT II
For Violation of Section 20(a) of the Exchange Act
Against the Individual Defendants

111. Plaintiff repeats and realleges each and every allegation contained in the foregoing paragraphs as if fully set forth herein.

112. The Individual Defendants acted as controlling persons of Zoom within the meaning of Section 20(a) of the Exchange Act. By virtue of their positions and their power to control public statements about Zoom, the Individual Defendants had the power and ability to control the actions of Zoom and its employees. By reason of such conduct, Defendants are liable pursuant to Section 20(a) of the Exchange Act.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

A. Determining that this action is a proper class action, designating Plaintiff as Lead Plaintiff and certifying Plaintiff as a Class representative under Rule 23 of the Federal Rules of Civil Procedure and Plaintiff's counsel as Lead Counsel;

B. Awarding compensatory damages in favor of Plaintiff and the other Class members against all Defendants, jointly and severally, for all damages sustained as a result of Defendants' wrongdoing, in an amount to be proven at trial, including interest thereon;

C. Awarding Plaintiff and the Class their reasonable costs and expenses incurred in this action, including counsel fees and expert fees; and

D. Awarding such equitable/injunctive or other relief as deemed appropriate by the Court.

JURY DEMAND

Plaintiff demands a trial by jury.

DATED: April 8, 2020

/s/ James M. Wagstaffe

WAGSTAFFE, VON LOEWENFELDT, BUSCH & RADWICK LLP
James M. Wagstaffe (#95535)
Frank Busch (#258288)
100 Pine Street, Suite 725
San Francisco, California 94111
Telephone: (415) 357-8900
Facsimile: (415) 357-8910
wagstaffe@wvbrlaw.com
busch@wvbrlaw.com

LABATON SUCHAROW LLP
Christopher J. Keller
Eric J. Belfi
Francis P. McConville
David J. Schwartz
140 Broadway
New York, New York 10005
Telephone: (212) 907-0700
Facsimile: (212) 818-0477
ckeller@labaton.com
ebelfi@labaton.com
fmcconville@labaton.com

dschwartz@labaton.com

Attorneys for Plaintiff Kim Brams