ROBERT C. SCHUBERT S.B.N. 62684
WILLEM F. JONCKHEER S.B.N. 178748
NOAH M. SCHUBERT S.B.N. 278696
KATHRYN Y. MCCAULEY S.B.N. 265803
SCHUBERT JONCKHEER & KOLBE LLP
Three Embarcadero Center, Suite 1650
San Francisco, California 94111
Telephone: (415) 788-4220
Facsimile: (415) 788-0161
rschubert@sjk.law
wjonckheer@sjk.law
nschubert@sjk.law
kmccauley@sjk.law

CHRISTIAN LEVIS (*pro hac vice* forthcoming)
HENRY KUSJANOVIC (*pro hac vice* forthcoming)
AMANDA FIORILLA (*pro hac vice* forthcoming)
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Telephone: (914) 997-0500
Facsimile: (914) 997-0035
clevis@lowey.com
hkusjanovic@lowey.com
afiorilla@lowey.com

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

LISHOMWA HENRY, individually and on behalf of all others similarly situated, Plaintiff, v. ZOOM VIDEO COMMUNICATIONS, INC., a Delaware corporation, Defendant.	Case No.: **CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL**

Plaintiff Lishomwa Henry ("Plaintiff") complains upon knowledge as to himself and his own actions and upon information and belief as to all other matters against Defendant Zoom Video Communications, Inc., ("Zoom" or "Defendant") as follows:

SUMMARY OF ALLEGATIONS

1. This action arises from Defendant's lack of adequate data privacy and security protections and disclosures to its users as part of providing its extremely popular videoconferencing software. Defendant has shared Plaintiff's and Class members' data with the widely popular social network, Facebook, without adequate disclosure, and has failed to protect its users' data from theft by neglecting to adhere to standard data privacy protocols and requirements.

2. As a provider of videoconferencing software, Defendant has greatly benefitted from the recent pandemic that has forced many Americans to work from home. Zoom stated that daily meeting participants increased from 10 million to 200 million between December 2019 and March 2020.[1]

3. While people utilize Zoom's software on their phones, laptops, or desktop computers, Zoom has been putting the data of millions of people at risk with poor data security protections.

4. As Zoom's platform has become more popular, there have been an increasing number of reports that have exposed problems with the platform which permit hackers to access users' web cameras, permit access to users' recorded videoconferences, permit access into live videoconferences, and even give hackers the ability to completely control users' computers or devices. Additionally, Zoom routes many of its conferences through servers located in The People's Republic of China, which subjects them to seizure by the Chinese government.

5. Zoom has also published misleading marketing claims and privacy policies while secretly taking advantage of users by sharing their personal data with third parties and putting their information at risk.

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

JURISDICTION AND VENUE

6. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C §1332(d), because the amount in controversy for the Class exceeds $5,000,000 exclusive of interest and costs, there are more than 100 putative class members defined below and minimal diversity exists because a significant portion of putative class members are citizens of a state different from the citizenship of Defendant.

7. This Court has general personal jurisdiction over Defendant because its principal place of business is in San Jose, California. Additionally, Defendant is subject to specific personal jurisdiction in this State because a substantial portion of the events and conduct giving rise to Plaintiff's claims occurred in this State.

8. Venue is proper in this District pursuant to 28 U.S.C. §1391(b), (c), and (d) because Defendant transacts business in this District; a substantial portion of the events giving rise to the claims occurred in this District; and because Defendant is headquartered in this District.

9. Intra-district Assignment: A substantial part of the events and omissions giving rise to the violations of law alleged herein occurred in the County of Santa Clara, and as such, this action may be properly assigned to the San Jose division of this Court pursuant to Civil Local Rule 3-2(c).

PARTIES

A. Plaintiff

10. Plaintiff Lishomwa Henry ("Plaintiff") is a natural person and citizen of the State of New York and a resident of Queens County.

B. Defendant

11. Defendant Zoom Video Communications, Inc., is a Delaware corporation with principal executive offices located at 55 Almaden Boulevard, San Jose, California 95113.

SUBSTANTIVE ALLEGATIONS

12. Zoom has provided its video communication platform for companies and individuals in the United States and many other countries throughout the world. While Zoom may provide software that is very easy to use, the company has been severely irresponsible in maintaining the security of its users' data.

13. By clicking "Join," users are trusting that Zoom will provide the necessary security to protect their personal information and the content of their Zoom sessions, however Zoom's rapid rise in popularity has exposed that, despite its dramatic increase in revenue, it has cut corners to an extreme degree in securing its platform.

I. Zoom Has Been Sharing iOS User Data With Facebook's Developer Kit

14. On March 26, 2020 it was reported by Motherboard that the Zoom app for iOS was sending information about its users to Facebook even if the users did not have a Facebook account.[2]

15. The report stated that the 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 ID created by the user's device, which companies can use to target a user with advertisements.

16. This sharing of user data with Facebook was not disclosed by Zoom's privacy policy. Zoom claims to protect its users' privacy, stating on its website "you trust us to connect you to the people that matter. We value that trust more than anything else. We want you to know what data we collect and how we use it to provide our service."[3]

17. Zoom's Privacy Policy purports to identify and disclose to its users all the information Zoom automatically collects from its users when they interact with Zoom products. Zoom's Privacy Policy states that it "utilize[s] a combination of industry-standard security technologies, procedures, and organizational measures to help protect your Personal Data from unauthorized access, use, or disclosure."

18. Zoom's failure to provide accurate disclosures to its users about sharing their data and failure to implement adequate security protocols violates its users' privacy and falls well short of Zoom's promises.

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

[3] http://zoom.us/privacy-and-legal

II. Zoom's Misleading Statements About End-to-End Encryption

19. Encryption is the method by which information is converted into secret code that hides the information's content and meaning. This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext. Only authorized parties can convert ciphertext back to plaintext and access the original information, generally through the use of a secure passcode.

20. End-to-end encryption is intended to prevent data from being accessed by anyone other than by the true sender and recipient. This means that the data is encrypted while being transmitted to the recipient and the platform provider does not have a means to decrypt it.

21. Zoom marketed itself as offering end-to-end encryption. But on March 31, 2020, The Intercept reported that Zoom appeared to employ a simpler form of security in which the data is encrypted when it is being accessed from the meeting endpoints, however the data passes through Zoom's central servers where it is decrypted before being re-encrypted and transmitted to the recipient.[4]

22. On April 1, 2020 Zoom published a blog post stating, "we want to start by apologizing for the confusion we have caused by incorrectly suggesting that Zoom meetings were capable of using end-to-end encryption," explaining that there are instances when Zoom will decrypt the communications of its users in certain circumstances such as when the when their cloud-based recording system is being used.[5] This would permit an attacker to redirect the data stream from a cloud-recording without breaking into the meeting.

23. It was also reported by security research organization Citizen Lab that Zoom uses a single shared key, or password, among all meeting participants and that the password is generated

[4] Micah Lee, Yael Grauer, *Zoom Meetings Aren't End-To-End Encrypted, Despite Misleading Marketing*, https://theintercept.com/2020/03/31/zoom-meeting-encryption/

[5] Oded Gal, *The Facts Around Zoom and Encryption For Meetings/Webinars*, https://blog.zoom.us/wordpress/2020/04/01/facts-around-zoom-encryption-for-meetings-webinars/

using a weak algorithm susceptible to cracking, and that the passwords are generated not by endpoints, but by company-run servers.[6]

III. Chinese Involvement

24. The Citizen Lab report also stated that they observed the transmission of meetings and encryption keys through servers in China. The Chinese government has the authority to compel companies to provide authorities access to their servers. The Citizen Lab report stated that, "Zoom may be legally obligated to disclose the encryption keys to authorities in China."[7]

25. Although Zoom is a Silicon Valley-based company, the report noted that Zoom owns three companies in China through which at least 700 employees are paid to develop Zoom's software.

26. This issue has been recently addressed by Congress. In November 2019, the United States Senate introduced a bill to curtail the flow of sensitive information about people in the U.S. to China through large tech companies that provide services to Americans. The bill, named The National Security and Personal Data Protection Act, subjects companies with ties to countries of "national security concern," including China, to a privacy regime that prevents the companies from collecting private data on U.S. users beyond what is required to run their services. This concern stems from Chinese laws that require companies to provide their data to Chinese intelligence services.[8]

27. Citizen Lab performed a test of a Zoom meeting with two users, one in the United States and one in Canada. They found that the encryption key was sent to one of the participants from a Zoom server located in Beijing. The report stated that, "[a] company primarily catering to

[6] Bill Marczak, John Scott-Railton, *Move Fast and Roll Your Own Crypto: A Quick Look at the Confidentiality of Zoom Meetings*, https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/

[7] Bill Marczak, John Scott-Railton, *Move Fast and Roll Your Own Crypto: A Quick Look at the Confidentiality of Zoom Meetings*, https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/

[8] Emily Birnbaum, *GOP senator introduces bill to limit flow of US data to China*, https://thehill.com/policy/technology/470860-gop-senator-introduces-bill-to-limit-flow-of-us-data-to-china

North American clients that sometimes distributes encryption keys through servers in China is potentially concerning, given that Zoom may be legally obligated to disclose th[o]se keys to authorities in China." *Id.*

28. The report concluded that, "[a]n app with easily-identifiable limitations in cryptography, security issues, and offshore servers located in China which handle meeting keys presents a clear target to reasonably well-resourced nation state attackers, including the People's Republic of China." *Id.*

IV. Recorded Meetings Are Not Secured And Easily Accessible on the Web

29. It was reported by the Washington Post on April 3, 2020, that videos recorded through Zoom's software were saved onto a separate online storage space without a password.[9]

30. Thousands of personal Zoom videos had been left viewable and unprotected, demonstrating the privacy risks to millions of Americans.

31. Zoom uses a standard naming convention for every video recording, therefore a simple online search reveals their recorded videos, available for anyone to access.

32. Videos viewed by The Washington Post included one-on-one therapy sessions, a training video for healthcare workers that included names and phone numbers, business meetings that included private company financial statements, and elementary school classes.

33. Zoom said in a statement that it "provides a safe and secure way for hosts to store recordings" and provides guides for how users can enhance their call security. "Should hosts later choose to upload their meeting recordings anywhere else, we urge them to use extreme caution and be transparent with meeting participants, giving careful consideration to whether the meeting contains sensitive information and to participants' reasonable expectations," the statement said. Five

[9] Drew Harwell, *Thousands of Zoom video calls left exposed on open Web*, https://www.washingtonpost.com/technology/2020/04/03/thousands-zoom-video-calls-left-exposed-open-web/

people identified in the videos The Washington Post viewed said they had no idea how the footage made its way online.[10]

34. Zoom videos are not recorded by default but call hosts can choose to record them and save to Zoom servers. It appears that calls are being recorded without the consent of chat participants.

35. Patrick Jackson, the technology chief of the privacy-software company Disconnect and a former researcher for the National Security Agency, who alerted The Post to the exposed data, said that he found the videos by using a free online search engine that scans through open cloud storage space online. One search for recordings using Zoom's default naming convention revealed more than 15,000 results.

V. Windows Security Risk

36. On March 31, 2020 Bleeping Computer published findings that Zoom lets attackers steal Microsoft Windows credentials.

37. When users share a hyperlink through the Zoom chat function, and when users click the link, Windows, by default, will send the user's login name and their password hash, which can be easily cracked using free tools like Hashcat to dehash and reveal the user's password.[11] A remote hacker could then gain complete access the users Windows computer.

38. Additionally, links sent over Zoom chat were able to launch programs on the recipient's computer without requesting permission from the user.

VI. Zoom Took Advantage of Users' Computers to Install its App

39. Evidence that Zoom has not taken cybersecurity seriously began to surface in mid-2019 when it was discovered that the mac operating system ("macOS") was vulnerable to having the video camera accessed by visiting a web page that loaded a malicious link.

[10] Drew Harwell, *Thousands of Zoom video calls left exposed on open Web*, https://www.washingtonpost.com/technology/2020/04/03/thousands-zoom-video-calls-left-exposed-open-web/

[11] Lawrence Abrams, *Zoom Lets Attackers Steal Windows Credentials, Run Programs via UNC Links*, https://www.bleepingcomputer.com/news/security/zoom-lets-attackers-steal-windows-credentials-run-programs-via-unc-links/

40. In mid-2019, a security researcher named Jonathan Leitschuh posted a report about security flaws with Zoom. The report noted that:

- The Zoom client app installed a Web server on the user's computer without disclosing it to the user.
- The Web server bypassed a security improvement in Safari designed to require users to click "Allow" each time a URL with an application-based link was loaded. Instead of prompting, the redirection was captured by Zoom's Web server, which launched the Zoom app without notifying the user.
- Zoom's Web server lacked basic security features, so an attacker can easily direct a user to a URL or load a URL within a Web page and trigger the Web server to join a Zoom meeting without any prompt. That allows an attacker to hear the user's audio and see the video through the user's video camera.
- If you removed the Zoom client app, Zoom's Web server remained in place and continued to run. If you subsequently clicked a link to join a Zoom meeting, the Web server would quietly and automatically reinstall and launch the Zoom client.

41. Leitschuh made his findings public on July 8, 2019.[12] After this disclosure Zoom removed the Web server from the install process and Apple added the Web server to its "malicious software" list.

42. On March 30, 2020, Daring Fireball's John Gruber published an article stating that Zoom's macOS installer bypasses the normal process in a standard installer noting that the installation happened in what is called the "preflight" process which permits the app to install without requiring user prompts to proceed. Gruber stated that this was "clearly not an oversight or honest mistake" and that "[i]t's a complete disregard for doing things properly and honestly on Zoom's part. There's no way to check what files will be installed, or where in the computer they will be installed, before their installer has gone ahead and installed them."[13] This was designed by Zoom to avoid disclosure and bypass user intent.

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

[13] John Gruber, *Regarding Zoom*, https://daringfireball.net/2020/03/regarding_zoom

VII. One of Zoom's Software Bugs Gave Hackers Full Control Over Computers

43. Former NSA hacker and security researcher Patrick Wardle revealed two security flaws that have been discovered and still did not have a fix, known as "zero-day exploits." These bugs are targeted by hackers because there is no way to defend an exploitation of the vulnerability.

44. If a hacker has access to control a computer, physically or remotely, they can add malicious code to the Zoom installer giving them full access to the entire computer. They can also inject code into the Zoom installation and get it to request that users provide the app access to the computer's camera and microphone, thereby providing the attacker with access to those features of the computer.[14]

VIII. Zoom's Software has Design Flaws That Allow Hackers Access to Private Videoconferences

45. One major design flaw by Zoom was having meeting IDs that were nine to eleven-digits in length. However, a nine to eleven-digit number is too small relative to the number of meetings being held. Security researchers at Check Point Research probed this weakness by writing a script that generated random numbers in the range Zoom employs and tested it on the Zoom platform. They found that 4% of the randomly generated numbers matched live meeting IDs. Check Point made its findings public on January 28, 2020.[15] This weakness is how a hacker can easily gain access to a private videoconference, known as "Zoombombing." Zoombombing is when an unauthorized person or stranger joins a Zoom meeting/chat session and causes disorder by saying offensive things and even photobombing your meeting by sharing pornographic and hate images.[16]

46. Zoom did not control the amount of times a user could request a Zoom meeting URL, a well-known technology function in the software industry, so the researchers were able to send thousands of URLs to Zoom's server and quickly determine which were actual life meetings.

[14] Patrick Wardle, *The 'S' in Zoom, Stands for Security: Uncovering (local) security flaws in Zoom's latest macOS client*, https://objective-see.com/blog/blog_0x56.html

[15] Alexander Chailytko, *Zoom-Zoom: We Are Watching You*, https://research.checkpoint.com/2020/zoom-zoom-we-are-watching-you/

[16] Kellep Charles, *What is Zoombombing and how to defend against it*, https://securityboulevard.com/2020/04/what-is-zoombombing-and-how-to-defend-against-it/

IX. Zoom Shared LinkedIn Data

47. On April 2, 2020, the New York Times reported that if a Zoom user had signed up for LinkedIn Sales Navigator, every Zoom participant's name and email address in the chat was matched against LinkedIn's database and, if they had a LinkedIn profile, they were connected to it. Any participant who subscribed to the LinkedIn feature could hover over a participant's name to see their LinkedIn profile card.

48. Zoom permanently removed the feature on April 1, 2020 after the New York Times contacted the company about it.

X. Zoom's Did Not Obtain User Consent Before Sharing Their Information

49. Zoom disclosed its users' information to undisclosed and unauthorized third parties without the users' consent.

50. The disclosure of a Zoom user's unique advertiser identifier is invasive because advertisers use this information to track data so they can deliver customized advertising. The identifier is used for tracking and identifying a user, allowing the advertiser to identify when users perform certain actions.

51. Advertisers use this information to learn more about users, including their behaviors, demographics and preferences. This information has significant economic value. Additionally, this information makes people more vulnerable to identity fraud.

52. Zoom's data-sharing activity was not visible to the user, thus Zoom users had no opportunity to express or withhold consent to Zoom's misconduct. Since they could not detect this activity, users of Zoom have no reasonable way of knowing whether their information will be safeguarded or disclosed without their consent.

53. Zoom users had no reason to expect that Zoom would transmit their information to undisclosed third parties without their consent to be used to track and target them.

XI. Zoom's Absolute Disregard For Standard Security Practices Put Zoom Users' Information at Risk and Ultimately Led to a Data Breach of Users' Credentials

54. Zoom's disregard for the security of its users' information put users at risk of identity theft and other dangers.

55. By cutting corners and by neglecting to spend the time, money, resources and effort to secure its platform, Zoom greatly increased the risk that its users would suffer harm.

56. In fact, Zoom users did suffer harm, as explained in a Forbes article published on April 13, 2020 titled, "500,000 Hacked Zoom Accounts Given Away For Free On The Dark Web."[17]

57. Cybersecurity researchers were able to contact some of the compromised account holders and they were told that the usernames and passwords found on the dark web were in fact correct. *Id.*

58. The various shortcomings in their programming that was described above were simply cost cutting measures to enable Zoom to maximize its bottom line at the expense of users' privacy and security.

59. Zoom is a for profit corporation that has been valued at over $30 billion dollars. With vast resources at its disposal, Zoom's failure to protect the welfare of its users which comprise private individuals and many United States government agencies is inexcusable.

60. A Forbes report revealed that U.S. agencies handling the coronavirus response had spent a collective $1.3 million on Zoom technology in just a few days at the end of March. Not only had the Centers for Disease Control and Prevention (CDC) and the Federal Emergency Management Agency (FEMA) spent hundreds of thousands on Zoom for COVID-19-related webinars and calls, but other government agencies had also purchased the technology. That included the State Department and one organization that was the alleged victim of a major Chinese hack, the Office of Personnel Management, in a breach that saw the private data of 21 million Americans leak. The U.K. government is also a well-known user of the tool, hosting critical cabinet meetings over Zoom.[18]

[17] Lee Matthews, *500,000 Hacked Zoom Accounts Given Away For Free On The Dark Web*, https://www.forbes.com/sites/leemathews/2020/04/13/500000-hacked-zoom-accounts-given-away-for-free-on-the-dark-web/#603da42c58c5

[18] Thomas Brewster, *Why Zoom Really Needs Better Privacy: $1.4 Million Orders Show The US Government's COVID-19 Response Is Now Relying On It*, https://www.forbes.com/sites/thomasbrewster/2020/04/02/why-zoom-really-needs-better-privacy-13-million-orders-show-the-us-governments-covid-19-response-is-now-relying-on-it/#5f30164977e8

61. Zoom's failure to take adequate measures to secure its users data is inexcusable and creates liability as described in the claims below.

CLASS ACTION ALLEGATIONS

62. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following Class:

> All individuals who used the Zoom platform in the United States during the time period of four years prior to the filing of the complaint through the present.[19]

63. Excluded from each Class are: (1) any Judge or Magistrate presiding over this action and any members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which Defendant or its parent has a controlling interest and their current or former employees, officers, and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

64. **Ascertainability:** Membership of the Class is defined based on objective criteria, and individual members will be identifiable from Defendant's records, including the Zoom accounts.

65. **Numerosity:** The exact number of members of the Class is unknown and unavailable to Plaintiff at this time, but individual joinder in this case is impracticable. The Class likely consists of thousands of individuals, if not millions of individuals, and the members can be identified through Defendant's records.

66. **Predominant Common Questions:** The Class' claims present common questions of law and fact, and those questions predominate over any questions that may affect individual Class members. Common questions for the Class include, but are not limited to, the following:

a. Whether Defendant violated Plaintiff's and Class members' privacy rights;

b. Whether Defendant acted negligently;

[19] Plaintiff has defined the Class based on currently available information and hereby reserves the right to amend the definition of the Class, including, without limitation, the Class Period.

c. Whether Defendant's acts and practices complained of herein amount to egregious breaches of social norms;

d. Whether Plaintiff and the Class members were harmed;

e. Whether Defendant and Plaintiff formed implied contracts;

f. Whether Defendant breached implied contracts with Plaintiff and the Class members;

g. Whether Defendant's conduct was unfair;

h. Whether Defendant's conduct was fraudulent;

i. Whether Defendant omitted or misrepresented material facts regarding the information of Plaintiff and Class members it shared with third parties, including Facebook;

j. Whether Plaintiff and the Class members are entitled to equitable relief, including but not limited to, injunctive relief, restitution, and disgorgement; and,

k. Whether Plaintiff and the Class members are entitled to actual, statutory, punitive or other forms of damages, and other monetary relief.

67. **Typicality:** Plaintiff's claims are typical of the claims of the other members of the proposed Class. Defendant's conduct that gave rise to the claims of Plaintiff and the members of the Class is the same for all members of the Class.

68. **Adequate Representation:** Plaintiff has and will continue to fairly and adequately represent and protect the interests of the Class. Plaintiff has retained counsel competent and experienced in complex litigation and class actions, including privacy violations. Plaintiff has no interest that is antagonistic to those of the Class, and Defendant has no defenses unique to Plaintiff. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the members of the Class, and they have the resources to do so. Neither Plaintiff nor his counsel have any interest adverse to those of the other members of the Class.

69. **Substantial Benefits:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single

adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

70. Plaintiff reserves the right to revise the foregoing class allegations and definitions based on facts learned and legal developments following additional investigation, discovery, or otherwise.

CALIFORNIA LAW APPLIES TO THE ENTIRE CLASS

71. California's substantive laws apply to every member of the Class, regardless of where in the United States the Class member resides. The State of California has sufficient contacts to Defendant's relevant conduct for California law to be uniformly applied to the claims of the Class. The application of California law to all relevant Class members comports with the Due Process Clause given the significant aggregation of contacts between Defendant's conduct and California.

72. Zoom is headquartered and does substantial business in California.

73. A significant percentage of the Class members are located in California and a substantial portion of Zoom's unlawful conduct was conducted in California.

74. The conduct that forms the basis for each Class member's claims against Zoom emanated from Zoom's headquarters in San Jose, California, including Zoom's misrepresentations and omissions regarding data privacy. Zoom instructs users with questions about privacy to contact Zoom at an address in San Jose.

75. California has a greater interest than any other state in applying its law to the claims at issue in this case. California has a strong interest in preventing its resident corporations from engaging in unfair and deceptive conduct and in ensuring that harm inflicted on resident consumers is redressed. California's interest in preventing unlawful corporate behavior occurring in California substantially outweighs any interest of any other state in denying recovery to its residents injured by an out of state defendant or in applying its laws to conduct occurring outside its borders.

76. The application of California laws to the Class is also appropriate under California's choice of law rules because California has significant contacts to the claims of Plaintiff and the proposed Class, and California has a greater interest in applying its laws here than any other interested state.

CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF

Negligence
(On Behalf of Plaintiff and the Class)

77. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

78. Defendant provided services to Plaintiff and the Class Members, including the ability to participate in videoconferences that Zoom marketed and represented as secured. Plaintiff's and the Class members' use of Zoom was predicated on the understanding that Zoom would take appropriate measures to protect their information. Zoom had a special relationship with Plaintiff and the Class members as a result of being entrusted with their content and information, which created a duty of care between Zoom and the Class.

79. Defendant owed a duty to Plaintiff and the Class to exercise reasonable care in implementing and maintaining reliable security systems and practices to ensure the safety of Plaintiff and the Class members' information by securing their information using reasonable and accepted methods, and by not disclosing, this information to third parties, like Facebook, without informed consent.

80. Defendant breached its duties by, failing to implement and maintain reasonable security protections for users and by disclosing personal user information to third parties, like Facebook, without the consent of its users.

81. But for Defendant's actions and breaches of its duties, Plaintiff's and Class members' information would be secure. Third parties, like Facebook, would not have gained access to users' information and users' Zoom credentials would not have wound up on the dark web for hackers to exploit.

82. It was foreseeable that Defendant's conduct as alleged herein would harm Plaintiff and the Class. Plaintiff knew or should have known that its inability to adequately protect user

information, and sharing information with third parties, like Facebook, would cause harm to Plaintiff and the Class.

83. Defendant's breach as alleged herein directly and proximately resulted in Plaintiff's and the Class' injuries.

84. As a result of Defendant's breach, Plaintiff and the Class have been damaged in the amount to be determined at trial.

SECOND CLAIM FOR RELIEF
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

85. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

86. Defendant offered its videoconferencing capabilities to Plaintiff and the Class Members. In exchange, Defendant received benefits in the form of monetary payments and access to Plaintiff's valuable personal information.

87. Defendant has acknowledged these benefits and accepted or retained them.

88. Implicit in the exchange of the products and services for the benefits provided by Plaintiff and the Class members is an agreement that Defendant would safeguard their personal information.

89. Without such implied contracts, Plaintiff and the Class members would not have conferred benefits on Defendant, but rather would have chosen an alternative videoconference platform that did not fail to protect their information, or intentionally share their information with undisclosed and unauthorized parties.

90. Plaintiff and Class members fully performed their obligations under their implied contracts with Defendant, but Defendant did not perform its obligations.

91. Defendant breached its implied contracts with Plaintiff and the Class Members when it failed to protect their information, and when it disclosed their information to unauthorized third parties like Facebook. These circumstances are such that it would be inequitable for Defendant to retain the benefits received.

92. As a direct and proximate result of defendant's breach of its implied contracts with Plaintiff and the Class members, Plaintiff and the Class members have suffered and will continue to suffer injury.

93. Had Plaintiff and the Class members known the truth about Zoom's failure to protect their information, and Zoom's undisclosed sharing of their information with third parties, they would not have entrusted their information to Zoom and would not have been willing to use, or pay for, Zoom's videoconferencing services.

94. Plaintiff and Class members did not receive the benefit of their bargain with Zoom because they paid for a value of services, either through information or a combination of their information and money, they did not receive the privacy protections that Zoom should have provided.

THIRD CLAIM FOR RELIEF
Violation of the California Consumer Privacy Act
Cal. Civ. Code § 1798.100 *et seq.*
(On Behalf of Plaintiff and the Class)

95. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

96. California's Consumer Privacy Act ("CCPA") protects consumers' personal information from collection and use by businesses without consumers' notice and consent.

97. Defendant violated the CCPA by using customers' information without providing the required notice under the CCPA. *See* Cal. Civ Code § 1798.100(b). Defendant did not notify Plaintiff and the Class members that it was disclosing their information to unauthorized parties.

98. Defendant also violated the CCPA by failing to provide notice to its customers of their right to opt-out of the disclosure of their information to unauthorized third parties. *See* Cal. Civ. Code § 1798.120(b). Defendant did not give Plaintiff and the Class members the opportunity to opt out before it provided their information to unauthorized parties.

99. Defendant further violated the CCPA by failing to adequately protect Plaintiff's and Class members' information from data breach, and to prevent Plaintiff's and Class members' unencrypted and unredacted personal information from unauthorized disclosure. This failure was a

result of Defendant's violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information of Plaintiff and Class members. *See* Cal. Civ. Code 1798.150(a).

100. As a direct and proximate result of the Defendant's acts, Plaintiff's and Class members' personal information was subjected to a data breach, and subject to unauthorized disclosure through the Zoom app where personal information was regularly collected and sent to third parties without authorization.

101. As a direct and proximate result of Defendant's acts, Plaintiff and the Class members were injured and lost money or property, including but not limited to the leak of their personal information in the data breach, along with information and/or the price received by Defendant for the services, the loss of the Class members' legally protected interest in the confidentiality and privacy of their personal information, nominal damages and additional losses.

102. Defendant knew or should have known that Zoom's security practices were inadequate to safeguard the Class members' personal information and that the risk of unauthorized disclosure was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

103. Plaintiff seeks injunctive relief in the form of an order enjoining Defendant from continuing to violate the CCPA, as well as statutory and actual damages on behalf of himself and the class.

104. Plaintiff has also provided written notice to Defendant identifying the specific provisions of the CCPA it has violated. If Defendant fails to respond to Plaintiff's notice letter or agree to adequately cure the violations described herein (and to certify that no further violations will occur), Plaintiff will also seek statutory damages on behalf of himself and the class.

FOURTH CLAIM FOR RELIEF
Violation of California Unfair Competition Law ("UCL")
Bus. & Prof. Code § 17200
(On Behalf of Plaintiff and the Class)

105. Plaintiff re-alleges and incorporates the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

106. California's UCL prohibits any "unlawful, unfair, or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising." *See* Cal. Bus. & Prof. Code § 17200.

107. Defendant engaged in unlawful activity prohibited by the UCL. The actions of Defendant as alleged herein constitute unlawful and unfair business practices within the meaning of the UCL.

108. Defendant's acts, as described herein, are "fraudulent" because they are likely to deceive the general public.

109. Defendant's business practices, as alleged herein, violate the "unfair" prong of the UCL because they offend established public policy and are immoral, unethical and unscrupulous or substantially injurious to consumers.

110. The reasons, justifications, or motives that Defendant may offer for the acts and omissions described herein are outweighed by the gravity of harm to the victims. The injuries suffered by Plaintiff and the Class members are substantial and are not outweighed by any countervailing benefits to consumers or competition.

111. Defendant's business practices described herein also violate the UCL because Defendant: falsely represented that its goods or services are of a particular standard when they are of another; advertised its goods or services with the intent not to sell them as advertised; falsely represented the subject of a transaction that was supplied, and made material omissions regarding its safeguarding of user information.

112. Had users, including Plaintiff, known the truth about Zoom's information sharing practices they would not have entrusted their information to Zoom and would not have been willing to use, pay for, or pay as much for, Zoom's products. As such, Plaintiff and class members did not receive the benefit of their bargain with Zoom because they paid for a value of services, either through information or a combination of information and money and did not receive the protections they expected.

113. As a result of Defendant's unfair business practices, Plaintiff and the Class members suffered injury.

FIFTH CLAIM FOR RELIEF
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

114. Plaintiff re-alleges and incorporate the preceding allegations of this Complaint with the same force and effect as if fully restated herein.

115. Defendant has profited and benefited from the use of its videoconferencing services by Plaintiff and the Class in exchange for monetary benefits and access to user information.

116. Defendant has voluntarily accepted and retained these benefits and profits with full knowledge and awareness that, as a result of the misconduct and omissions described herein, Plaintiff and the Class members did not receive products of the quality, nature, fitness or value represented by Defendant and that reasonable consumers expected.

117. Defendant has been unjustly enriched by its withholding and retention of these benefits at the grave expense of plaintiff and the Class Members.

118. Equity and justice prohibit Defendant from retaining these profits and benefits.

119. Plaintiff and the Class members suffered injury as a direct and proximate result of Defendant's unjust enrichment and seek an order directing Defendant to disgorge these benefits and pay restitution to Plaintiff and the Class members.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff on behalf of himself and the proposed Class respectfully requests that the Court enter an order:

A. Certifying the Class and appointing Plaintiff as Class Representative;

B. Finding that Defendant's conduct was unlawful as alleged herein;

C. Awarding such injunctive and other equitable relief as the Court deems just and proper;

D. Awarding Plaintiff and the Class members statutory, actual, compensatory, consequential, punitive, and nominal damages;

E. Awarding Plaintiff and the Class members pre-judgment and post-judgment interest;

F. Awarding Plaintiff and the Class members reasonable attorneys' fees, costs, and expenses; and

G. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury for all issues so triable.

Dated: April 17, 2020

SCHUBERT JONCKHEER & KOLBE LLP

/s/Willem F. Jonckheer
Willem F. Jonckheer

ROBERT C. SCHUBERT S.B.N. 62684
NOAH M. SCHUBERT S.B.N. 278696
KATHRYN Y. MCCAULEY S.B.N. 265803
SCHUBERT JONCKHEER & KOLBE LLP
Three Embarcadero Center, Suite 1650
San Francisco, California 94111
Telephone: (415) 788-4220
Facsimile: (415) 788-0161
rschubert@sjk.law
wjonckheer@sjk.law
nschubert@sjk.law
kmccauley@sjk.law

LOWEY DANNENBERG, P.C.
CHRISTIAN LEVIS (*pro hac vice* forthcoming)
HENRY KUSJANOVIC (*pro hac vice* forthcoming)
AMANDA FIORILLA (*pro hac vice* forthcoming)
LOWEY DANNENBERG, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
Telephone: (914) 997-0500
Facsimile: (914) 997-0035
clevis@lowey.com
hkusjanovic@lowey.com
afiorilla@lowey.com

LOWEY DANNENBERG, P.C.
Anthony M. Christina (*pro hac vice* forthcoming)
One Tower Bridge
100 Front Street, Suite 520
West Conshohocken, PA 19428
Tel.: (215) 399-4770
Fax: (914) 997-0035

achristina@lowey.com

Attorneys for Plaintiff

CIVIL COVER SHEET

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

I. (a) PLAINTIFFS

Lishomwa Henry, individually and on behalf of all others similarly situated,

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

Queens County, NY

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

Schubert Jonckheer & Kolbe LLP
3 Embarcadero Center, Suite 1650
San Francisco, CA 94111

Telephone: (415) 788-4220

DEFENDANTS

f ZOOM VIDEO COMMUNICATIONS, INC., a Delaware corporation,

County of Residence of First Listed Defendant Santa Clara, CA
(IN U.S. PLAINTIFF CASES ONLY)

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

Attorneys *(If Known)*

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

☐ 1 U.S. Government Plaintiff

☒ 3 Federal Question *(U.S. Government Not a Party)*

☐ 2 U.S. Government Defendant

☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

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

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☒ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

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

CONTRACT

- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment Of Veteran's Benefits
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☒ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY

- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY

- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury -Medical Malpractice

CIVIL RIGHTS

- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities–Employment
- ☐ 446 Amer. w/Disabilities–Other
- ☐ 448 Education

PERSONAL INJURY

- ☐ 365 Personal Injury – Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY

- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

PRISONER PETITIONS

HABEAS CORPUS

- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

OTHER

- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee– Conditions of Confinement

FORFEITURE/PENALTY

- ☐ 625 Drug Related Seizure of Property 21 USC § 881
- ☐ 690 Other

LABOR

- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION

- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY

- ☐ 422 Appeal 28 USC § 158
- ☐ 423 Withdrawal 28 USC § 157

PROPERTY RIGHTS

- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent─Abbreviated New Drug Application
- ☐ 840 Trademark

SOCIAL SECURITY

- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS

- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS–Third Party 26 USC § 7609

OTHER STATUTES

- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC § 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced & Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

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

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

VI. CAUSE OF ACTION

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

Brief description of cause:

VII. REQUESTED IN COMPLAINT:

☑ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, Fed. R. Civ. P.

DEMAND $

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

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

JUDGE

DOCKET NUMBER

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

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

DATE 4/17/20

SIGNATURE OF ATTORNEY OF RECORD s/ Willem F. Jonckheer

Print Save As... Reset

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS-CAND 44

Authority For Civil Cover Sheet. The JS-CAND 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I. a) Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

b) County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

c) Attorneys. Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)."

II. Jurisdiction. The basis of jurisdiction is set forth under Federal Rule of Civil Procedure 8(a), which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.

(1) United States plaintiff. Jurisdiction based on 28 USC §§ 1345 and 1348. Suits by agencies and officers of the United States are included here.

(2) United States defendant. When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.

(3) Federal question. This refers to suits under 28 USC § 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.

(4) Diversity of citizenship. This refers to suits under 28 USC § 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked**.** (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)

III. Residence (citizenship) of Principal Parties. This section of the JS-CAND 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. Nature of Suit. Place an "X" in the appropriate box. If the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerk(s) in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.

V. Origin. Place an "X" in one of the six boxes.

(1) Original Proceedings. Cases originating in the United States district courts.

(2) Removed from State Court. Proceedings initiated in state courts may be removed to the district courts under Title 28 USC § 1441. When the petition for removal is granted, check this box.

(3) Remanded from Appellate Court. Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.

(4) Reinstated or Reopened. Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.

(5) Transferred from Another District. For cases transferred under Title 28 USC § 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.

(6) Multidistrict Litigation Transfer. Check this box when a multidistrict case is transferred into the district under authority of Title 28 USC § 1407. When this box is checked, do not check (5) above.

(8) Multidistrict Litigation Direct File. Check this box when a multidistrict litigation case is filed in the same district as the Master MDL docket.

Please note that there is no Origin Code 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

VI. Cause of Action. Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC § 553. Brief Description: Unauthorized reception of cable service.

VII. Requested in Complaint. Class Action. Place an "X" in this box if you are filing a class action under Federal Rule of Civil Procedure 23.

Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.

Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. Related Cases. This section of the JS-CAND 44 is used to identify related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

IX. Divisional Assignment. If the Nature of Suit is under Property Rights or Prisoner Petitions or the matter is a Securities Class Action, leave this section blank. For all other cases, identify the divisional venue according to Civil Local Rule 3-2: "the county in which a substantial part of the events or omissions which give rise to the claim occurred or in which a substantial part of the property that is the subject of the action is situated."

Date and Attorney Signature. Date and sign the civil cover sheet.