SUPERIOR COURT OF THE DISTRICT OF COLUMBIA
CIVIL DIVISION

CONSUMER WATCHDOG, individually and on behalf of the general public, 413 E. Capitol St., SE, First Floor, Washington, D.C. 20003, *Plaintiff*, v. ZOOM VIDEO COMMUNICATIONS, INC., a Delaware corporation, 55 Almaden Boulevard, 6th Floor, San Jose, California 95113, *Defendant*.	Case No.: **JURY TRIAL DEMANDED**

COMPLAINT

Plaintiff Consumer Watchdog ("Plaintiff" or "Consumer Watchdog") brings this Complaint and Demand for Jury Trial on behalf of the general public against Defendant Zoom Video Communications, Inc. ("Defendant" or "Zoom") for making false and deceptive representations to consumers about its data security practices in violation of the District of Columbia Consumer Protection Procedures Act ("CPPA"), D.C. Code § 28-3901, *et seq.* Plaintiff, for its Complaint, alleges as follows:

NATURE OF THE ACTION

1. As the number of reported data breaches and privacy incidents continues to soar, consumers are making data security a crucial consideration when choosing which companies to do business with and which products to buy. In fact, according to a recent Harris Poll survey, data security is "not just an under-the-hood operational function, it is part of how companies are

judged in the consumer marketplace."[1] Many businesses are therefore investing in data security technologies and distinguishing themselves by offering stronger data security features than their competitors. According to Jay Cline, the United States ("U.S.") Privacy Leader at PricewaterhouseCoopers, "[m]arkets are ready to be disrupted by companies who can get this right[.]"[2]

2. Zoom is positioned within an extremely saturated workplace collaboration market. To distinguish itself from competitors and attract new customers, Zoom began advertising and touting its use of a strong security feature called "end-to-end encryption" to protect communications on its platform, meaning that the *only* people who can access the communicated data are the sender and the intended recipient. Using end-to-end encryption prevents unwanted third parties—including the company that owns the platform (in this case, Zoom)—from accessing communications, messages, and data transmitted by users.

3. In certain industry sectors, this level of data security is not just desired, but also necessary to protect vulnerable populations and comply with regulatory privacy laws. For example, the healthcare industry takes particular care in selecting communication platforms that are secure enough to comply with the Health Insurance Portability and Accountability Act ("HIPPA").

4. Zoom repeated its end-to-end encryption claims throughout its website, in white papers—including in its April 2020 HIPAA Compliance Guide—and on the user interface within

---

[1] IBM, *IBM Cybersecurity and Privacy Research,* https://newsroom.ibm.com/Cybersecurity-and-Privacy-Research (last accessed Aug. 10, 2020).

[2] N.F. Mendoza, *Data privacy: What consumers want businesses to know*, TechRepublic*,* https://www.techrepublic.com/article/data-privacy-what-consumers-want-businesses-to-know/ (last accessed Aug. 10, 2020).

the app. Through these representations, Zoom established itself as a safe, secure, and reliable video conferencing platform for consumers, and targeted sectors that require highly secure communication systems.

5. Further, there is no question that consumers—and businesses in the healthcare sector—have specifically relied on Zoom's false end-to-end encryption representations. For example, one large telehealth company explained its decision to deliver its services through Zoom's platform as follows:

> Zoom offers an end-to-end encryption which is leveraged during communication . . . [Company] inherits this encryption during all video conferencing between patients and Care Team personnel. [Company] ensures that the end-to-end encryption is enabled as part of the package for the Remote Patient Monitoring, designed to facilitate HIPAA based compliance requirements.

6. Unfortunately, Zoom's claims that communications on its platform were end-to-end encrypted were false. Zoom only used the phrase "end-to-end encryption" as a marketing device to lull consumers and businesses into a false sense of security.

7. The reality is that Zoom is, and has always been, capable of intercepting and accessing any and all of the data that users transmit on its platform—the very opposite of end-to-end encryption. Nonetheless, Zoom relied on its end-to-end encryption claim to attract customers and to build itself into a publicly traded company with a valuation of more than $70 billion.

8. By falsely promising consumers that their video calls would be protected with end-to-end encryption, Zoom blatantly violated the CPPA, D.C. Code § 28-3904, which prohibits unlawful and deceptive trade practices.

9. To make matters worse, numerous reports suggest that while Zoom holds itself out as an American company, it nonetheless maintains servers in China, has meaningful ties to the People's Republic of China, currently employs more than 700 employees in China that work

in "research and development[,]" and may have disclosed its American users' sensitive personal information to the Chinese government.[3] In fact, U.S. Senators Richard Blumenthal (D-Conn.) and Josh Hawley (R-MO.) have recently urged the Department of Justice ("DOJ") to investigate Zoom for reported violations of Americans' civil liberties, as well as the national security implications of its relationships with the People's Republic of China.[4]

10. Accordingly, Plaintiff brings this suit on behalf of the general public and the tens of thousands of District of Columbia ("D.C.") consumers to seek redress for Zoom's unlawful and deceptive conduct. Plaintiff seeks civil penalties, restitution, and all necessary, appropriate, and available equitable and injunctive relief to address, remedy, and prevent harm to D.C. residents resulting from Zoom's misconduct.

PARTIES

11. Plaintiff Consumer Watchdog is a 501(c)(3) non-profit, public benefit corporation with offices in Washington, D.C., located at 413 E. Capitol St., SE, First Floor, Washington, D.C. 20003 and California, located at 6330 South San Vicente Blvd Suite 250, Los Angeles, California 90048. Consumer Watchdog is a nationally recognized non-partisan, non-profit corporation dedicated to representing the interests of taxpayers and consumers through advocating and fighting false advertising and corporate deception, and protecting consumers' online data security and privacy.

12. Defendant Zoom is a corporation existing under the laws of the State of Delaware,

---

[3] 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/ (last accessed Aug. 10, 2020).

[4] U.S. Senators Richard Blumenthal and Josh Hawley, *Letter to Assistant Attorney General John C. Demers*, https://www.blumenthal.senate.gov/imo/media/doc/07.30.20%20-%20DOJ%20-%20China%20Investigations.pdf (last accessed Aug. 10, 2020)

with its headquarters and principal place of business located at 55 Almaden Boulevard, 6th Floor, San Jose, California 95113. Zoom conducts business throughout Washington, D.C.

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction over Defendant pursuant to D.C. Code §§ 11-921 and 28-3905.

14. This Court has personal jurisdiction over Defendant pursuant to D.C. Code § 13-423 because Zoom conducts significant business in D.C., solicits contracts in D.C., enters into contracts to supply services in D.C., and because the unlawful conduct causing injury alleged in this Complaint occurred by its acts and omissions in D.C.

FACTUAL BACKGROUND

I. Zoom's Business Model and Recent Success.

15. Zoom is a publicly traded company that provides remote video conferencing services for businesses and individuals.

16. While based in San Jose, California, the company also has sales and account management employees in other cities around the U.S. and the world, including Washington, D.C. The company also markets its services to individuals in D.C. and provides services to tens of thousands of D.C. residents.

17. Founded in 2011, the company grew its user base over the course of several years and achieved a $1 billion valuation by 2017. Zoom went public on the NASDAQ in March 2019 and, at the end of its initial public offering, was valued at just under $16 billion. Zoom is currently valued at over $70 billion.

18. By January 2020, Zoom had attracted millions of users to its service platform, which can be accessed through users' laptops, desktops, and the Zoom mobile app for Apple and

Android devices.

19. In recent months, Zoom's use among consumers has skyrocketed in conjunction with the national response to the COVID-19 pandemic. According to CNBC, Zoom's user base has grown to 12.92 million monthly active users, a twenty-one (21) percent increase since the end of 2019.[5]

20. As Zoom's user base has grown, so has its valuation. Since February 21, 2020—when many other stocks started to crash as the pandemic became more severe—Zoom's stock has more than doubled in value.[6]

21. Zoom users have—as relevant here—two options for how to use the app. They may use the free version of Zoom, which places a forty-minute limit on the maximum duration of a video conference, among other restrictions. Otherwise, they may use Zoom through one of several paid plans, which contain fewer limits and additional features, for prices ranging from $14.99 per month to $19.99 per month.[7] (Zoom also provides a variety of other paid options as well, including a healthcare-focused version for $200 per month.)

22. Zoom's growth in popularity has seen an increased focus on the platform's security, as many public and private organizations are using Zoom to communicate and conduct day-to-day business. Recent media reports have described a growing trend of "Zoombombing[,]" in which third parties obtain the credentials to join a Zoom call in order to disrupt the call by,

---

5 Jordan Novet, *Zoom has added more videoconferencing users this year than in all of 2019 thanks to coronavirus, Bernstein says*, https://cnb.cx/2WWnewd (last accessed Aug. 10, 2020).

6 Jeremy Bowman, *Is It Too Late to Buy Zoom Video Communications Stock?*, The Motley Fool, https://www.fool.com/investing/2020/06/16/is-it-too-late-buy-zoom-video-communications-stock.aspx (last accessed Aug. 10, 2020).

7 Zoom, *Zoom Meeting Plans for Your Business*, https://zoom.us/pricing (last accessed Aug. 10, 2020).

e.g., depicting swastikas and making racially offensive comments.[8]

23. However, these problems pale in comparison to a core deficiency in Zoom's security—one that remains in place to this day and which the company has itself acknowledged.

II. Zoom Promised End-To-End Encryption of Video Calls But Didn't Provide It.

24. Consistently and across multiple mediums, Zoom has claimed that its video conferencing platform supported "end-to-end encryption[.]" It has said this in a Security White Paper published in June 2019, as well as on its website since at least October 28, 2018.[9] It has highlighted how "end-to-end encrypted Zoom allows" a federal regulatory authority to work securely while using the platform.[10] And it has even suggested that, at least as to its healthcare-focused clients, for "video conferencing, the . . . security architecture must provide end-to-end encryption and meeting access controls so data in transit cannot be intercepted."[11] (*See also* Figures 1, 2, and 3.)

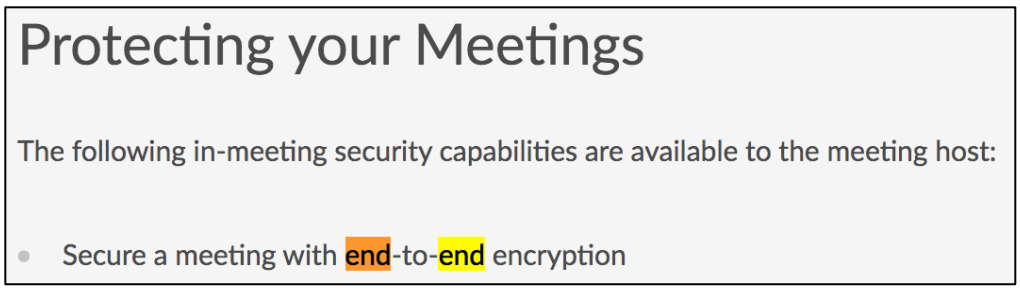
---

[8] Salvador Hernandez, *A Zoom Meeting For Women Of Color Was Hijacked By Trolls Shouting The N-Word*, BuzzFeed News, https://bit.ly/2R1C8NG (last accessed Aug. 10, 2020).

[9] Zoom, *Security at Zoom*, https://zoom.us/security (last accessed July 30, 2020) ("The following in-meeting security capabilities are available to the meeting host . . . Secure a meeting with encryption[.]"); Zoom, *Zoom Meetings & Chat*, https://web.archive.org/web/20181028201834/https://www.zoom.us/meetings (last accessed August 10, 2020 via Internet Archive).

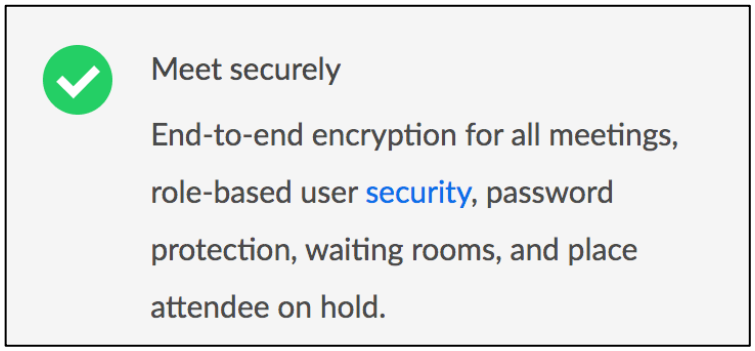
[10] Rena Gadimova, *End-to-End Encrypted Zoom Allows FINRA to Maintain a High-Security Posture*, Zoom Blog https://bit.ly/3dJIfjy (last accessed Apr. 10, 2020). (Article's name has since been changed to "Zoom Allows FINRA to Maintain a High-Security Posture" (last accessed Aug. 10, 2020).)

[11] Zoom, *HIPAA Compliance Guide*, https://web.archive.org/web/20200401043011/https://zoom.us/docs/doc/Zoom-hipaa.pdf (last accessed July 30, 2020 via Internet Archive); *see also* 45 CFR §§ 164.312(a)(2)(iv), (e)(2)(ii).



(Figure 1.)

(Figure 2.)

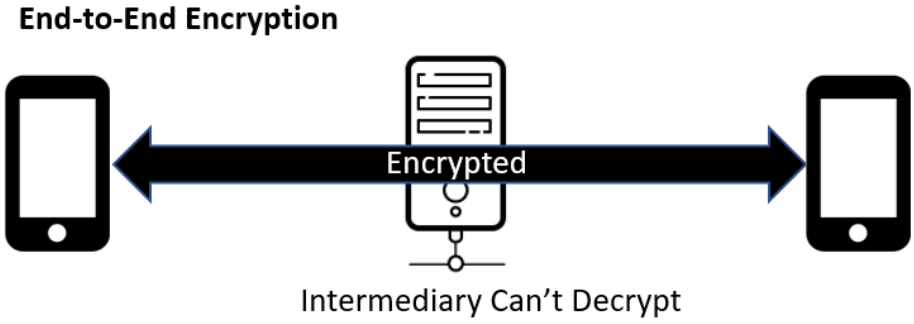


(Figure 3.)

25. The company's claim of providing end-to-end encryption was false.

26. "[E]nd-to-end encryption" is defined in Federal Standard 1037 (superseded by American National Standard T1.523-2001) as "[t]he encryption of information at its origin and decryption at its intended destination without any intermediate decryption."[12]

27. With end-to-end encryption, data passes through the service provider's intermediate servers, but encryption and decryption are handled strictly by the parties of the communication. Therefore, the parties' communications are kept private from not only outside attackers, but also from the service provider itself. (*See* **Figure 4**.)



(Figure 4.)

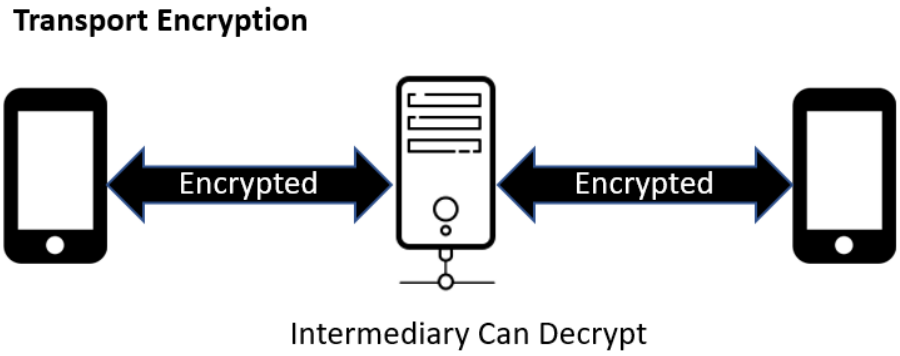
28. Instead of using end-to-end encryption as explicitly advertised, Zoom uses what is known as "transport encryption" or "Transport Layer Security" ("TLS") where data transmitted over the service must also pass through Zoom's servers—but now can be read and/or collected by Zoom itself. As described by a recent article in *The Intercept*, "[t]he encryption that Zoom uses to protect meetings is TLS, the same technology that web servers use to secure HTTPS websites."[13] While TLS can be used to protect communications in transit between a party and

---

[12] These standards provide departments and agencies of the Federal government with a comprehensive source of definitions for various telecommunications related terms.

[13] Micah Lee & Yael Grauer, *Zoom Meetings Aren't End-To-End Encrypted, Despite Misleading Marketing*, Intercept, https://theintercept.com/2020/03/31/zoom-meeting-encryption/ (last accessed Aug. 10, 2020).

Zoom's servers from attackers, it does not prevent Zoom from decrypting and accessing the communications' content as it passes though Zoom's intermediate servers. (*See* **Figure 5**.)



(Figure 5.)

29. The difference between "end-to-end" and "transport" encryption is significant. Users on Zoom's platform utilize the service with the belief that no one outside of an individual video conference session can see or hear the information being transmitted or otherwise learn about the conference. Given that individuals and companies use Zoom to discuss and share confidential trade secrets, it is particularly troubling that Forbes recently reported that some Zoom conversations were being routed through servers in China—a country whose government is often accused of trade secret theft.[14] In fact, U.S. Senators Richard Blumenthal (D-Conn.) and Josh Hawley (R-MO.) have recently urged the Department of Justice to open an official investigation into Zoom over its reported violations of American civil liberties, including reports that it may have disclosed private information about Americans to the People's Republic of China.[15]

---

[14] Thomas Brewster, *Warning: Zoom Makes Encryption Keys In China (Sometimes)*, Forbes, https://www.forbes.com/sites/thomasbrewster/2020/04/03/warning-zoom-sends-encryption-keys-to-china-sometimes/#71d359a53fd9 (last accessed Aug. 10, 2020).

[15] *Supra* n.4.

30. Therefore, Zoom's advertised end-to-end encryption feature was particularly important given that many (in D.C. and elsewhere) are now spending significant amounts of personal time communicating over Zoom and sharing sensitive information on the platform. Security is thus of paramount concern, and many customers using Zoom's free and paid services have used the platform without knowing that Zoom can monitor transmissions on the back end.

31. Notably, in response to *The Intercept* article, Zoom *admitted* that its encryption is not truly end-to-end. Zoom's Chief Product Officer Oded Gal later wrote a blog post in which he apologized on behalf of the company "for the confusion we have caused by incorrectly suggesting that Zoom meetings were capable of using end-to-end encryption."[16]

32. Zoom's admission—and its platform's shortcoming—is even more striking because end-to-end encryption *could* have been set up for a video conferencing platform like Zoom. For instance, Apple's FaceTime application uses end-to-end encryption. As a Johns Hopkins University computer science professor noted to *The Intercept*, "if it's all end-to-end encrypted, you need to add some extra mechanisms to make sure you can do that kind of 'who's talking' switch, and you can do it in a way that doesn't leak a lot of information. You have to push that logic out to the endpoints . . . It's doable."

33. These promises for enhanced platform security come only after facing backlash over its falsely advertised claims of end-to-end encrypted video conferencing. Upon information and belief, Zoom has been warned of its platform's deficiencies by privacy advocates. As the Center for Democracy and Technology's former Privacy & Data Project Director Michelle De Mooy recently stated, she and others "have spoken to Zoom over the past few years and made

---

[16] Oded Gal, *The Facts Around Zoom and Encryption for Meetings/Webinars*, Zoom Blog https://bit.ly/3dVwJBX (last accessed July 30, 2020).

them aware of glaring privacy and security concerns that they did little to correct."[17]

34. Following revelations surrounding Zoom's security deficiencies, many entities began preventing its use. New York City—despite being the nation's largest COVID-19 hotspot *and* largest school district by enrollment—forbid the use of Zoom for remote learning.[18] The New York Attorney General has similarly raised concerns about Zoom's privacy practices and started to investigate.[19] Even Elon Musk's "rocket company SpaceX has banned its employees from using video conferencing app Zoom, citing 'significant privacy and security concerns[.]'"[20]

THE INTERESTS OF CONSUMER WATCHDOG & THE GENERAL PUBLIC

35. Plaintiff Consumer Watchdog acts for the benefit of the General Public as a private attorney general pursuant to D.C. Code § 28-3905(k)(1).

36. Since 1985, Consumer Watchdog has worked diligently representing the interests of consumers through advocating and fighting against corporate deception and false advertising. A core focus of Consumer Watchdog's advocacy is its Privacy and Technology project, which seeks to protect consumers' online privacy and enable consumers to regain control over data about them.[21]

37. Plaintiff focuses its efforts on consumer protection and advocacy, including

---

17 Michelle De Mooy, LinkedIn; *Michelle De Mooy*, Ctr. for Democracy & Tech., https://cdt.org/staff/michelle-de-mooy/ (last accessed Apr. 6, 2020).

18 Alex Zimmerman, *NYC forbids schools fromuUsing Zoom for remote learning due to privacy and security concerns*, Chalkbeat, https://bit.ly/2JKazEM (last accessed Aug. 10, 2020).

19 Danny Hakim & Natasha Singer, *New York Attorney General Looks Into Zoom's Privacy Practices*, https://nyti.ms/2Rgo2s3 (last accessed Aug. 10, 2020).

20 Munsif Vengattil & Joey Roulette, *Elon Musk's SpaceX Bans Zoom Over Privacy Concerns –Memo*, https://reut.rs/2JF78z4 (last accessed July 30, 2020).

21 *See* Consumer Watchdog, Privacy and Technology, https://www.consumerwatchdog.org/privacy-technology (last accessed Aug. 10, 2020).

efforts to ensure the safe and secure use of online services and platforms.

38. Upon information and belief, tens of thousands of D.C. residents use Zoom regularly for video conferencing and communication.

39. Seeking to tap into increased consumer demand for private and secure forms of online communication, Zoom falsely advertised end-to-end encryption as a standard security feature for its video conferencing service.

CAUSE OF ACTION
Violations of the D.C. Consumer Protection Procedures Act
(On Behalf of the General Public and D.C. Consumers)

40. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

41. This Count is brought by Consumer Watchdog on behalf of the General Public and D.C. consumers pursuant to D.C. Code §§ 28-3905(k)(1)(C) and (D).

42. Pursuant to D.C. Code § 28-3905(k)(1)(C), "[a] nonprofit organization may, on behalf of itself or any of its members, or on any such behalf and on behalf of the general public, bring an action seeking relief from the use of a trade practice in violation of a law of the District[.]"

43. Pursuant to D.C. Code § 28-3905(k)(1)(D), "a public interest organization may, on behalf of the interests of a consumer or a class of consumers, bring an action seeking relief from the use by any person of a trade practice in violation of a law of the District if the consumer or class could bring an action under subparagraph (A) of this paragraph for relief from such use by such person of such trade practice."

44. The CPPA is a remedial statute that is to be broadly construed. Its purpose is to assure that a just mechanism exists to remedy all improper trade practices and in order to deter the continuing use of such practices.

45. D.C. Code § 28-3904 prohibits any person from engaging in unfair and deceptive, "whether or not any consumer is in fact misled, deceived, or damaged thereby," including by:

(a) "represent[ing] that goods or services have a source, sponsorship, approval, certification, accessories, characteristics, ingredients, uses, benefits, or quantities that they do not have[,]" *id.* § 28-3904(a);

(b) "represent[ing] that goods or services are of particular standard, quality, grade, style, or model, if in fact they are of another[,]" *id.* § 28-3904(d);

(c) "misrepresent[ing] as to a material fact which has a tendency to mislead[,]" *id.* § 28-3904(e);

(d) "fail[ing] to state a material fact if such failure tends to mislead[,]" *id.* § 28-3904(f);

(e) us[ing] innuendo or ambiguity as to a material fact, which has a tendency to mislead[,]" *id.* § 28-3904(f-1); and

(f) "advertis[ing] or offer goods or services without the intent to sell them or without the intent to sell them as advertised or offered[,]" *id.* § 28-3904(h).

46. The CPPA's jurisdiction extends beyond the unlawful trade practices listed in D.C. Code § 28-3904 to practices that are prohibited by any statute, regulation, common law, or other law of the District of Columbia.

47. Merchants who violate the CPPA may be recover treble damages, or $1,500 per violation, whichever is greater, payable to the consumer; attorney's fees; punitive damages; an injunction; and, in representative actions, any additional relief as necessary to restore to the consumer money or property. D.C. Code §§ 28-3905(k)(2)(A)-(E).

48. Zoom is a merchant because, in the ordinary course of its business, it sells and supplies consumer services directly to consumers and its video communication service is a

consumer service within the meaning of D.C. Code § 28-3901(a)(7).

49. Zoom has engaged in conduct that constitutes unlawful and deceptive trade practices by making deceptive representations about the nature of the encryption provided for video communications on its platform to the public, including to D.C. residents, and falsely claiming that it provided end-to-end encryption. D.C. Code §§ 28-3904(a), (d)-(f-1), (h). False claims about data security and encryption are routinely found to be deceptive, including by the Federal Trade Commission. *See, e.g.*, *In the Matter of James V. Grago, Jr., individually and d/b/a ClixSense.com*, 2019 WL 1932143, at *1 (F.T.C. April 24, 2019).

50. Zoom's statements about the security and privacy of its services—including statements claiming that it provided end-to-end encryption and that its security architecture prevents data and communications from being intercepted—are material and have the tendency to mislead consumers and are unlawful trade practices that violate the CPPA, D.C. Code § 28-3904(f-1).

51. Zoom intended that the public, including D.C. residents, rely on its deceptive claims and representations regarding the security of communications on its platform.

52. Rather than provide the level of encryption it publicly and repeatedly promised, Zoom chose to provide something less: a video communication platform where communications can be viewed, accessed, and disclosed by Zoom at any time.

53. Although reliance is not required by the CPPA, consumers have nevertheless reasonably relied on Defendant's uniform misrepresentations and omissions when using and purchasing its video communication service.

54. Accordingly, Plaintiff seeks all damages available at law, including statutory damages to each and every D.C. consumer who used and/or purchased access to Zoom's video

communication service, injunctive relief prohibiting Zoom from misrepresenting its privacy and security policies, reasonable attorneys' fees and costs, and such other relief as deemed appropriate.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Consumer Watchdog, individually and in its representative capacity on behalf of the general public and the interests of D.C. consumers, prays for the following relief:

(A) Declare that Defendant's actions, as described herein, violate the D.C. Consumer Protection Procedures Act, D.C. Code §§ 28-3904(a), (d)-(f-1), (h);

(B) Award all appropriate injunctive relief as necessary to protect the interests of Plaintiff, the interests of consumers, and the General Public, including, among other things, an order prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

(C) Award damages including:

i. the greater of (a) treble damages, or (b) statutory damages in the amount of $1,500 per violation, pursuant to D.C. Code § 28-3905(k)(2)(A);

ii. additional relief as may be necessary to restore consumer money or property, real or personal, which may have been acquired by means of Defendant's unlawful trade practice, pursuant to D.C. Code § 28-3905(k)(2)(E); and

iii. Punitive damages, where applicable, to Plaintiff, the general public, and a class of D.C. Consumers in an amount determined at trial, pursuant to D.C. Code § 28-3905(k)(2)(C);

(D) Award Plaintiff reasonable litigation expenses and attorneys' fees, pursuant to

D.C. Code § 28-3905(k)(2)(B);

(E) Award Plaintiff and members of the General Public pre- and post-judgement interest to the extent allowable; and

(F) Award such other and further relief as equity and justice may require, pursuant to D.C. Code § 28-3901(k)(2)(F).

JURY DEMAND

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

Respectfully submitted,

CONSUMER WATCHDOG, individually and on behalf of the general public,

Dated: August 10, 2020

By:/s/_____
One of Plaintiff's Attorneys

Harvey Rosenfield
harvey@consumerwatchdog.org
CONSUMER WATCHDOG
413 E. Capitol St., SE, First Floor
Washington, D.C. 20003
D.C. Bar No. 295915

*Jerry Flanagan
jerry@consumerwatchdog.org
*Benjamin Powell
ben@consumerwatchdog.org
CONSUMER WATCHDOG
6330 San Vicente Blvd., Suite 250
Los Angeles, California 90048
Tel: 310.392.0522

*Jay Edelson
jedelson@edelson.com
*Ari J. Scharg
ascharg@edelson.com
*Theo J. Benjamin
tbenjamin@edelson.com
EDELSON PC
350 North LaSalle Street, 14th Floor

Chicago, Illinois 60654
Tel: 312.589.6370
Fax: 312.589.6378

*Admission *pro hac vice* to be sought