fieldfisher

Confidential
Stichting Onderzoek Marktinformatie (SOMI)
Attn. mr. Drs. H.J.M.G. Franke
PO Box 59692
1040 LD Amsterdam

Amsteldijk 220
1079 LK Amsterdam
Netherlands

T +31 20 2252200

www.fieldfisher.com

Also via e-mail to: info@somi.nl

Our ref: AVN/AVN/NL01-000813-00001/90715277 v1

Ady van Nieuwenhuizen
Partner
+31 (0)2 022 52 220 (Direct)
+31 (0)657 053 957 (Mobile)
ady.vannieuwenhuizen@fieldfisher.com

Amsterdam, 1 October 2020

Dear Mr. Franke

With reference to our letter of 31 August 2020, we can inform you as follows. We have been able to review and discuss the letter of 14 July 2020 ("**Letter**") with Zoom. Zoom disagrees with SOMI's allegations that it might infringe the Dutch implementation of the General Data Protection Regulation ("**AVG**") in various fashions. We appreciate the concerns that SOMI expresses, but we will explain below why these concerns are not necessary as there might be some misunderstanding about Zoom's systems, technology and data protection practices.

At a high level, we will note the following in response to SOMI's allegations:

- **Encryption**: Zoom has used AES-256 encryption for certain kinds of data, and now (with the release of Zoom 5.0 earlier this year), uses AES-256 for audio, video, and application sharing (i.e., screensharing, whiteboarding) in transit between Zoom applications, clients, and connectors. Zoom's past statements that it employs "end-to-end encryption" were accurate because Zoom meeting data was encrypted end-to-end in transit from one Zoom end client to every other Zoom end client and Zoom has not developed tools that would have actually enabled it to decrypt meeting data in real time.

- **Vulnerabilities**: Over the past year, the press has reported (often inaccurately) several alleged vulnerabilities in Zoom's software. All software platforms must remediate bugs and correct vulnerabilities, and Zoom is no different. Overall, the vulnerabilities identified by SOMI largely presented only theoretical and remote risk. Zoom closed the vulnerabilities swiftly after it learned of and validated the issues, as has been acknowledged in the same public reports relied upon by

SOMI. Zoom denies that the reported instances in which Zoom credentials were allegedly traded on the "dark web" occurred as a result of any breach of Zoom systems.

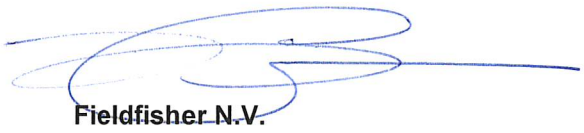
- **SDKs**: Zoom, like many companies, uses third party software development kits ("**SDKs**") to enhance its services and enable various functions desired by its users. The information associated with the Facebook SDK was not sensitive or confidential, and Zoom's use of the Facebook SDK (or any other SDK) was not wrongful.

- "**ZoomBombing**": As has been publicly reported, malicious third party actors have sometimes been able to disrupt Zoom meetings if the meeting host publicly posts the meeting link without enabling a password (or if the host shares the password publicly). As such, this phenomenon did not result from vulnerability in Zoom's software or a security breach.

In general, SOMI's contention that Zoom is insufficiently transparent about and attentive to its users' security and privacy is unfounded. Zoom, like many software companies, continuously improves its security measures, and communicates transparently with the public about these measures. For more information, please review the information available on Zoom's website: *zoom.us/docs/en-us/privacy-and-security.html*.

We look forward to hearing from you with any further questions or concerns.

Yours sincerely



Fieldfisher N.V.

Marcel Willems

Ady van Nieuwenhuizen