Philip C. Swain (SBN 150322)
pswain@foleyhoag.com
FOLEY HOAG LLP
155 Seaport Boulevard
Boston MA 02210
Telephone: 617-732-1000
Facsimile: 617-832-7000

Attorneys for Non-Party Joe Security, LLC

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

FINJAN, INC.

Plaintiff,

vs.

JUNIPER NETWORKS, INC.

Defendant.

Case No. C 17-05659 WHA

SECOND DECLARATION OF STEFAN BUEHLMANN IN SUPPORT OF MOTION TO FILE UNDER SEAL (DKT 513)

I, Stefan Buehlmann, hereby state the following under oath:

1. I live in Witterswil, Switzerland.

2. I am the General Manager of Joe Security LLC ("Joe Security").

3. Joe Security is a Swiss entity located in Reinach, Switzerland.

4. I have been involved in computer security and malware detection for 15 years.

5. Joe Security is in the computer security business. Specifically, Joe Security has developed a malware analysis and detection system, called the Joe Sandbox system that enables users to detect and analyze computer viruses and malware threats.

6. We carefully screen our customers and only license our product to reputable governmental security agencies and select corporations. The total number of Joe Security customers is limited. Our customer list is confidential.

7. All of our business and governmental partners agree to strict confidentiality restrictions as a condition of using our solution.

8. Our customers install our solution into their computer infrastructure to help protect against malware threats.

9. Juniper Networks, the defendant in this case, is one of our customers.

10. In his deposition dated February 7, 2019, Khurram Islah, a software developer for Juniper Networks described the technical details of Joes Security's Joe Sandbox system. The testimony and descriptions of the Joe Sandbox system in the Islah deposition are trade secrets and highly confidential information of Joe Security.

11. As a company that focuses on computer malware, we know that the efficacy of our product could be immediately, directly and completely compromised if the information in the Islah deposition is made public. Hackers would be able to use this information to modify their malware to circumvent our malware detection and prevention system.

12. We would prefer that no part of the Islah deposition be made public. Public disclosure of the descriptions and technical details in the deposition would compromise the efficacy of our malware prevention product.

13. In the event that the Court declines to allow the deposition sealed in its entirety, we would request the opportunity to redact the confidential references (although I estimate the redactions would be substantially more than 50% of the deposition transcript).

I declare under the pains and penalties of perjury that the foregoing is true and correct this 7th day of June, 2019.

Stefan Buehlmann