SANDVINE

February 16, 2018

Michael H. Wilson
University of Toronto – Chancellor
Office of the Chancellor
University of Toronto
27 King's College Circle, Room 206
Toronto, ON Canada M5S1A1

Meric Gertler
University of Toronto – President
Office of the President
University of Toronto
27 King's College Circle, Room 206
Toronto, ON Canada M5S1A1

Professor Ronald Deibert
Director, The Citizen Lab
Munk School of Global Affairs
University of Toronto
315 Bloor Street West
Toronto, ON Canada M5S 0A3

Dear Messrs. Wilson, Gertler, and Deibert:

The purpose of this letter is to respond to the claims made in the letter signed by Professor Deibert on behalf Citizen Lab at the University of Toronto dated February 12, 2018 and attached hereto, that our Company's product, PacketLogic, was used to inject malicious software, FinFisher spyware, ads, and cryptocurrency mining viruses. These claims are false, misleading, and technically inaccurate. We have never had, directly or indirectly, any commercial or technology relationship with FinFisher or any surveillance technology vendors, and our products do not, and cannot, inject malicious software. As explained below, we have strong safeguards in place regarding social responsibility, human rights, and privacy rights, and your allegations to the contrary are unfounded.

Following my initial email communication to Mr. Diebert, I learned that he notified several news outlets of your allegations prior to allowing us an opportunity to respond and outline the inaccuracies in the February 12 letter. Your February 12 letter stated that you would "appreciate" a response to your letter on or before February 20. I promptly replied to your letter on February 13 and stated that we would provide you with a more detailed response in the near term. Ignoring this, you shared your baseless allegations with members of the media which resulted in harm to Sandvine. Set forth below are several examples of why the allegations in your letter are false, misleading, and wrong.

Examples of Statements and Conclusions in Your Letter That Are False, Misleading, and Wrong

As is standard in the industry, our customer contracts contain confidentiality clauses which prevent us from disclosing the existence of or details about any specific customer contract and use case. Notwithstanding this fact, we can share the following relative to your claims.

First and foremost, *PacketLogic is* ***not capable of Man-In-The-Middle (MITM) attacks and not capable of any form of payload injection, malicious or not***. PacketLogic implements redirection with a 307 redirect packet, per an industry standard approach and specification referenced under Internet Engineering Task Force (IETF) standard RFC7231. The design of PacketLogic does not permit the end user to inject a payload larger than 1 packet.

Given PacketLogic's lack of payload injection capabilities, ***the claims made in your letter that PacketLogic was used "to inject traffic on a mass scale" to inject spyware, FinFisher, ads, and cryptocurrency mining viruses are false and the conclusions you arrived at are wrong.*** Moreover, were it even technically feasible, any such injection of a malicious payload would be prohibited as a matter of the Company's Business Ethics Committee (BEC) policy as further outlined herein and the terms of the EULA.

Content filtering and HTTP redirection are common and widely deployed technologies for beneficial and lawful use enabled by Sandvine through PacketLogic and dozens of other technology vendors' products. As you are well aware, common use cases for content filtering existing across enterprise, telecom service providers, and regulatory markets include traffic management and efficiency, parental controls, blocking of illegal content (*e.g.*, child pornography), digital rights enforcement of pirated content, and endpoint security. Similarly, HTTP redirection is commonly used for subscriber self-care and notification of when and why content is blocked (*e.g.*, a redirect to operator portal).

Further, you state in your letter that you, the University of Toronto and/or Citizen Lab, procured a "second-hand PacketLogic device". A review of our order book indicates no formal license purchase or contract with The Citizen Lab or University of Toronto. Your admission that you acquired and used our product violates our EULA, the terms of the contract with the original licensee, as well as other applicable laws. Our contracts expressly prohibit resale or transfer of our products. This restriction is intended, among other things, to ensure that our product is not used by third-parties in ways which would violate our ethical use policies, BEC review, and export controls. Please return the product to us immediately, and confirm that you intend to do so by reply email.

Sandvine Has A Comprehensive Business Ethics Program

Contrary to the claims in your letter, we take the ethical use of our product seriously. Since I became CEO of Procera and Sandvine, we have enhanced our ethics processes and product technology controls. By way of example, in early 2016, Procera Networks established a Business Ethics Committee (BEC) to review and approve the sale of products and services to customers. The BEC uses best practices based on a variety of factors, including, for example, global indices related to human rights and knowledge of intended use cases to identify the risk of product misuse prior to the sale of our products. Please refer to our website for additional detail on our Ethics Policy and BEC (www.sandvine.com/company/corporate-ethics). The BEC has been in operation continuously since its inception and has denied a number of potential customers access to the product. Adoption of this same ethics framework and processes was initiated immediately upon close of the Sandvine purchase in 2017. We also have been implementing the same controls regarding our software license into Sandvine products. Additionally, Sandvine has numerous other corporate and social responsibility policies in place (Code of Conduct, ISO14001, Environmental Policy, and Accessibility Policy).

In addition to the BEC, the Company's end user license agreement (EULA) expressly prohibits the use of PacketLogic to violate privacy rights. As part of our BEC process, we may decide to terminate the EULA and the right to use the software for any violation of our EULA. Finally, Sandvine implements stringent software license controls that limit access to specific product capabilities outside of an intended use case.

In summary, contrary to the allegations made in your letter, we have robust practices, procedures, and contractual requirements concerning social responsibility, human rights, and privacy rights.

In closing, I have and will continue to encourage transparent, fact-based collaboration with interested stakeholders. However, any public statements that the University of Toronto and/or Citizen Lab makes against Sandvine that are factually inaccurate or based on improper use of our product, such as the claims made in your letter, will be met with vigorous fact-based rebuttal and a strong legal response against the individuals and organizations that have made them.

Respectfully,

Lyndon Cantor
CEO
Sandvine
e: lcantor@sandvine.com

cc:

Steve Moate
Senior Legal Counsel
University of Toronto
Simcoe Hall
27 King's College Circle, Room 112
Toronto ON Canada M5S1A1
c/o: Stacie.Ozdemir@utoronto.ca
416-946-7794