[stamp:]

Filed with the Clerk on

NOV.10, 2016

PROSECUTOR'S OFFICE

OLIVER CIRIC
LAWYER AT THE GENEVA BAR
Tel: +41 (0)22 888 2000
Fax. +41 (0)22 888 2010
oliver.ciric@gmail.com

Prosecutor's Office
Attn.: Mr. Olivier Jornot
Attorney General
6B, route de Chancy
CP 3565
1211 Geneva 3

Geneva, November 10, 2016

Re.: Criminal complaint filed by Global Risk Profile Sarl

Mr. Attorney General,

Please be informed that I have been mandated by Global Risk Profile Sarl (*Société à responsabilité limitée* [Limited Liability Company]) who is hereby filing a criminal complaint regarding the facts as described herein. My law office has been selected as the service address. The procuration granted to me is included as document 6 of the criminal complaint.

Thank you in advance for taking the action within your power with regards to the present.

Yours sincerely,

[signature]
Olivier Ciric, Attorney at Law

Encl. Mentions

Global Risk Profile Sarl
Avenue des Communes-Réunies 47
1212 Grand-Lancy

Mr. Olivier JORNOT
Attorney General
Prosecutor's Office
6B, Route de Chancy
1213 Petit Lancy

November 10, 2016

Mr. Attorney General

The undersigned, Global Risk Profile Sarl ("Global Risk Profile" or "GRP") is obliged to file a criminal complaint with your office regarding the offenses which will be described below.

We hereby declare that we are filing as the complainant. Our Attorney is Mr. Olivier Ciric, whose offices are at 54, quai Gustave-Ador, 1207 Geneva (document 6).

The facts which will be described below concern the unauthorized access to a computer system (art. 143bis of the Criminal Code), the removal of data (Article 143 CC) and the deterioration of data (Article 144bis CC).

Additionally, the examination of the complaint will show that the acts described therein were committed in Switzerland within the meaning of Art. 3 CC, i.e. either that the acts themselves were committed on Swiss territory or that the results occurred there, in accordance with Art. 8, para. 1 CC. Finally, we wish to point out that Global Risk Profile is a Swiss company to which Art. 7 CC is thus fully applicable in any case.

The documents appended to the present complaint are frequently in English. In fact, we have opted to produce them in this language to avoid translation fees, but naturally if translation to French should be required with respect to certain aspects, we have instructed our Attorneys to do what is necessary.

Having made this preliminary introduction, we would hereby like to present the following:

Facts:

1. Global Risk Profile is a Geneva-based company specializing in research, due diligence, and information analysis and processing (Document 1).

2. On Sunday October 16, 2016, in the course of a routine monitoring activity regarding the use of the Global Risk Profile name, one of Global Risk Profile's employees discovered a blog article entitled "Dark Web hackers offer up confidential customer data from Global Risk Profile hack" (link: http://geekslop.com/2016/global-risk-profile-hacked-customer-data-dump) (document 2).

3. This article was written by a certain Brian Haddock and published online on September 27, 2016 in his blog *Geek slop* based in Texas in the United States (the address provided in the "About" section was as follows: 2345 Charles Ave., Burleson, TX 76028) (document 3).

4. In his article, Brian Haddock stipulated that a notable hacking group operating on the Dark Web[1] was selling data from Global Risk Profile, including confidential emails allegedly exchanged between Global Risk Profile and its clients. There follows a brief description about the company activities, which is false and "dramatized" and includes the order process via the client section (document 2).

5. According to the author, GRP had not informed its clients of the intrusion, at least not publicly; moreover, he stated that his attempts to contact Global Risk Profile had been ignored. As to the nature of the compromised data, Mr. Haddock presumed it was personal data (document 2).

6. To illustrate the content, Mr. Haddock used the Global Risk Profile logo without permission, to which he added a "thumbs down" and this in spite of the fact that this logo is an integral part of our graphic charter and is protected by copyright, in accordance with the footnote on our website (document 2).

7. On September 28, the blog article was disseminated on the content curation platform Scoop.it, also based in the United States (with its office at the following address: 48 2nd Street, 3rd Floor, San Francisco, CA 94108 United States) (document 3).

8. Additionally, since mid-October we have observed that the position of the article is improving in the Google search engine results associated with any search in relation to the Global Risk Profile name. Indeed, the article was on the fourth page when it was discovered whereas on November 8th the article appeared on page 2 (document 4).

9. As of Monday October 17th, we began to investigate the allegations set out in the abovementioned article. During our investigation, the link inviting Dark Web users to buy Global Risk Profile data was found; however, the link description contains no further information on the nature and volume of the data allegedly stolen (document 5).

10. Our investigation also revealed that Mr. Haddock had made an attempt to contact us on the very day the article was published, i.e. on September 27, through our contact form which was filled in under the name "Anonymous", which was why it was not taken into consideration.

Along with this investigation, we undertook the following actions:

11. On Monday, October 17, 2016, we carried out a check of the desktop and laptop computers belonging to the company.

12. On Monday, October 17, 2016, we also contacted our Internet provider in Geneva, Penta SA (*Société Anonyme* [Limited Company]), to request an analysis of the logs and any possible unauthorized or illegal access.

[1] "Dark Web" is an expression which designates internet content that can only be accessed with specific software and permissions. The "dark web" is often used for all types of illegal trafficking (drugs, data piracy, hardcore pornography, etc.).

13. On Tuesday, October 18, 2016, we mandated a company specializing in IT security, High-Tech Bridge SA, Geneva, to perform a full audit of our web and CRM sites (including the client section, which is fully included in the CRM that is directly accessible from our website), with the aim of revealing any vulnerabilities. In addition to this audit, a forensic analysis was also performed by the same company on Friday, November 2, 2016 (document 7).

14. Based on the results obtained (ImmuniWeb reports (document 8) and forensic analysis (document 7)), it was possible to establish the following facts:

15. This analysis revealed that since August 31, 2016, several targeted attacks were recorded on the Global Risk Profile website. As these attacks were specifically directed against our site, it can be affirmed that Global Risk Profile was directly targeted. Indeed, we have the confirmation that two companies mandated hackers to infiltrate our systems and thus illegally obtain data belonging to Global Risk Profile.

16. The security audit also revealed several vulnerabilities at the level of our client section. It is therefore possible that all of the data in the client section was compromised following the exploitation of one of these failures for illegal purposes.

17. The security audit also revealed that several of these attacks had a recurring IP address located in India (document 7).

18. The Global Risk Profile associate and president, Mr. Nicolas Giannakopoulos, is currently in dispute with SoftBank, based in Japan and in the United States, and more specifically with the former president of SoftBank United States, Nikesh Arora (who was obliged to resign in July 2016 due to the revelations brought forward by Mr. Giannakopoulos), as well as with his assistant, Mr. Alok Sama, who is still in office at SoftBank.

19. According to several informed sources, foreign investigation agencies have been mandated to make inquiries about Mr. Nicolas Giannakopoulos and damage his interests.

20. This information comes mainly from India and the United States. The former country is where Mr. Nikesh Arora was born and the latter is his country of residence.

21. We find it highly suspicious that the attacks began several weeks after Mr. Nikesh Arora had been "retired" from his position as CEO (the highest paid in the world, i.e. USD 500 million for less than a year in office) and one or two weeks after Mr. Giannakopoulos had been informed that individuals connected with the SoftBank had mandated a security company based in Great Britain to investigate him, his activities and his family.

22. The different cyber attacks committed against Global Risk Profile as well as the blog article with its clearly defamatory statements could thus be part of a more global attempt to harm Mr. Giannakopoulos's reputation and image, of which GRP would inevitably, and perhaps intentionally, be a collateral victim.

23. We also note that according to the information provided by Mr. Giannakopoulos, the abovementioned investigation agency is known for its dangerous and highly unethical behavior towards both its targets and its clients.

24. Furthermore, Mr. Giannakopoulos does not exclude the possibility that SoftBank itself or individuals within said multinational company are behind this clumsy attack. Indeed, a letter targeting the allegedly illegal behavior of Mr. Alok Sama, Mr. Arora's partner and "protégé", was sent to the SoftBank Board in Tokyo by Mr. Giannakopoulos's American attorney, Mr. Guirgis of Mintz & Gold in New York, on August 25, 2016, i.e. only five days prior to the first attacks against the Global Risk Profile website (document 9).

25. This is therefore a clear violation of Mr. Giannakopoulos's private sphere which leads us to fear the worst for his family and especially his children.

Based on the foregoing, we would be grateful if you would undertake the necessary investigations in order to find the persons guilty of this cyber attack as well as those who ordered it done, as soon as possible and with the utmost severity.

For Global Risk Profile Sarl:

[signature]

Nicolas Giannakopoulos

November 10, 2016

LIST OF DOCUMENTS

for

GLOBAL RISK PROFILE Sarl

1. Extract from the Registre du Commerce [Trade Registry] for Global Risk Profile Sarl
2. Article "Dark Web hackers offer up confidential customer data from Global Risk Profile hack"
3. Extract from the *"Geek slop"* blog
4. Google search page using the keywords "Global Risk Profile"
5. Offer to buy information hacked from Global Risk Profile
6. Procuration granted to Mr. O. Ciric
7. Forensic analysis
8. ImmuniWeb reports