Executive Vice-President of the
EU Commission
Margrethe Vestager (EUROPE FIT FOR A DIGITAL AGE)
margrethe-vestager-contact@ec.europa.eu

Joint Cybercrime Action Taskforce (JCAT)
Europol
P.O.Box 90850
2509 LW The Hague
The Netherlands

Vienna, July 14th, 2020

Dear Ms. Vestager!

Reference: Support for Cybercrime Victims!

1 The European Funds Recovery Initiative (EFRI) has been established in 2018 and by now represents more than 820 consumers who have been exploited by Investment scams[1] with an accumulated loss of more than EUR 34.7 million.

[1] In the context of this paper, we refer to websites that offer investments either unlicensed or licensed to European private investors. As alleged fraud models and / or investment scams, these websites violate both the ESMA restrictions (ban on selling to private investors, ban on binary options, ban on bonuses, etc.) as well as the licensing terms of the respective regulatory authorities. These fraud models usually do not segregate customers' accounts, nor are customers' funds actually invested through licensed exchanges or brokers, or even at all. For these investment scams, there is usually a large number of customer complaints and / or criminal complaints from investors, and / or investigations by the responsible law enforcement authorities are already pending, and / or warnings from financial regulators are already issued. This applies, for example, to online trading websites such as Option888 (no license), HandelFX (no license) or AlgoTechs / Bealgo (no license). Such fraud models are characterized by the fact that withdrawals are denied, payments to customers do not take place, or only partially, and after persistent complaints, and where the money invested by these private investors is transferred directly to offshore jurisdictions.

2 As our members – cybercrime victims – had to learn the hard way by losing their life savings, the increasing digitisation of society in general and the associated virtualisation of money in particular bring with them a new, massive threat to consumers - transnational cybercrime. The combination of state-of-the-art technologies with new marketing methods and a massive disparity in the technology affinity of Internet users is creating an unprecedented ecosphere for criminals.

3 We know that there are thousands of European victims who, like our members, who have lost their life savings to mafia-like Cybercriminals.

4 All our members have relied on working jurisdiction and law enforcement measures in the first place. Moreover, they trusted that the authorities ensure a safe cyber-environment as well as a safe online financial market, within their consumer environment as promised by our local and European authorities.

5 Our victims realise that, although governments seek to promote digitalization and to eliminate cash and enhance the online payment industry, neither local nor European law enforcement know how to appropriately address cybercrime. State-of-the-art technology mixed with criminal energy requires effective training and experience to successfully combat this phenomenon on the part of the authorities. At this point in time, with the EU cybersociety being at the early stage of the learning curve, our victims have had to pay a high price – their life savings – to learn this.

6 We are addressing you now with this Open Letter to draw your attention to the cybercrime court case currently underway in Vienna concerning the alleged Israeli cybercrime principal, Gal Barak. Mr Barak is, of course, subject to the presumption of innocence just like any other EU citizen. However, the victims of the various scams have already been publicly assigned with blame in the court room.

Criminal proceedings going on in Vienna, Austria

7 In January 2019, Austrian law enforcement agents in close cooperation with their EU colleagues were able to arrest suspected cybercriminals who systematically targeted EU consumers with their financial scams. This is certainly a major break-through in the EU transnational fight against cybercrime.

8 Currently, this trial in Vienna against the alleged principal of a vast EU cybercrime organization is the first in the EU. Hence, we take this trial in Vienna to draw your attention and that of the EU public to its importance of precedence.

9 Scammers like the Israeli Gal Barak have been running their scams through various offshore and shell companies in various jurisdictions. With their borderless and cross-jurisdictional methods, they have so far eluded criminal prosecution by the authorities and side-stepped the financial market supervisory authorities.

10 The trial of Gal Barak, therefore, can be considered to be a landmark in the fight against cybercrime throughout the EU. Once again, there is the presumption of innocence but also the obligation of the court to seek the truth.

More details on the trial

11 The charges against the Israeli GAL BARAK were brought after almost two years of investigation by the Austrian prosecution authorities in close cooperation with authorities of other European countries.

12 On 8 July 2020, the main hearing in the case against the Israeli citizen, Gal Barak, started in Vienna presided over by Judge Christian Böhm (LG 122 Hv 4/20g).

13 Barak stands publicly accused by the Prosecutor's Office of serious commercial fraud as well as money laundering by running investment scams. Barak is only one of more than a dozen suspects in this criminal case, but for procedural reasons he is currently the only defendant. He was arrested in February 2019 on the legal grounds of an EU arrest warrant in Bulgaria, where he and his wife Marina Barak (formerly Marina Andreeva) operated the company, E&G Bulgaria EOOD in Sofia.

14 Gal Barak was, together with his partners, the Russian Vlad Smirnov and the Israeli Gary "Gabi" Shalon, the beneficial owner of fraudulent online trading websites such as *XTraderFX*, *SafeMarkets*, *OptionStarsGlobal*, *Golden Markets,* or *CryptoPoint*. Together with his wife, the Bulgarian citizen Marina Barak, Gal Barak was not only responsible for the management of the illegal boiler rooms (call centres) in Bulgaria, Serbia and Montenegro, but also for the laundering of stolen money. He established a payment scheme using countless shell companies and illegal but also licensed payment processors such as Payvision and Wirecard.

Fraud with online trading websites

15 Fraud perpetrated on online trading websites (also known as investment scams or broker scams) has exponentially increased to an immense extent and with increasing digitalisation, especially in Europe. Estimates speak of losses of up to EUR 12 billion annually caused by this type of crime among unsuspecting small investors and consumers.

16 The approach to this type of online fraud can also be summarized as follows, based on the statements in the indictment against Gal Barak:

- Victims are acquired either through advertising on social media or by calls from boiler room agents.
- These call-centre employees present themselves as highly professional experienced securities traders and provide false identities and/or credentials. However, they often already know about the personal and financial circumstances of the prospective victim, as these data have been purchased. These Boiler Room agents are psychologically trained in advance, and they work according to precise instructions or scripts developed by sociologists and psychologists.
- After the first small deposits, the victims are given a verbal, but also visual, suggestion that it is possible for them to invest profitably in binary options, Forex or cryptocurrencies by increasing the balances on their online accounts.
- Through daily phone calls, their professional appearance and skilful requesting of more personal data, a close personal relationship is established between the Boiler Room employee and victim, and thus a relationship of trust is established, which leads to the customer depositing even more money.
- However, there are never any pay-outs of the allegedly high profits. After a while, the victims are told that all the money is just lost.

.

17 Motivated mainly by this confidence building to gain personal trust, tens of thousands of customers in Europe were deceived by Barak's Boiler Room agents into depositing more than EUR 200 million over a total period of 2 years.

18 In fact, the money deposited by the customers was never used to trade financial instruments, but was used to pay the service providers involved (Boiler Room employees, software providers, marketing service providers, advertising service providers, etc.) to the tune of 75%, and the remaining 25% of the victims' deposits was used by the scammers to finance their luxury and expensive lifestyles.

19 Once the victims had lost their money, they then had (and have) to experience that law enforcement and courts are not able to help them. They had to realize the issues and the barriers, and the inability of European law enforcement and prosecution to combat cybercrime. Evidently, criminal investigation into and prosecution for cybercrime is hindered and restricted by national borders, while cybercriminals do not have those restrictions.

Victims are just dumb and are loving the thrill

20 It is the duty and constitutional obligation of a defence lawyer to use all legally permitted means to protect his clients from conviction. However, he may not criminalise the victims or accuse others against his better knowledge and evidence.

21 In his opening plea on 8 July 2020, Barak's defence counsel, Dr. Peter Lewisch - partner in one of the most expensive law firms in Vienna - emphasised, as expected, the innocence of his client, who, incidentally, turns out to be without assets. In fact, the victims themselves were to blame, Lewisch explained in his plea. Only dumb or "stupid" people would believe the advertisements on the social media or the promises made by Boiler Room agents, and thereby it is irrelevant that they use stage names, as the “stupid” people would believe anything.

22 Lewisch went on to say that it really wasn't about investments or online trading, but about betting, i.e. gambling similar to a lottery. "People love the thrill, that's why they would do this.”

23 If one accepts this view as a statement in court, the path towards a cybersociety or towards a cashless society cannot be taken. Then, any fraud against a consumer would indirectly be blamed on the consumer himself. How can we then expect citizens to live cashlessly, shop online or do online banking?

Our request to you:

24 Unfortunately, cybercrime is often still considered a minor offence in the consumer sector. In fact, cybercrime endangers digital civil society and its basic values, as people are losing their life savings and are forced to face poverty in their old age.

25 We are convinced that It is the responsibility of the Member States, their courts, and law enforcement as a whole, to fight this kind of cybercrime with all means at their disposal. There must be zero tolerance in this regard.

26 Having said this, we further believe that cybercrime trials in individual countries should be closely followed and monitored by the EU in order to gain experience and to implement measures based on such precedents, to review current measures as well as introduce future directives or initiatives in the fight against cybercrime.

27 We know the principle of making the victim a perpetrator or an accomplice from the law on sexual offences. Until recently, victims of rape, coercion or sexual harassment were at least presented as complicit. Only the recent reforms to criminal law have begun to eliminate discrimination. Now, it seems that the victims of financial transactions must

also follow this path. At least Dr. Peter Lewisch tries to take this route of discrimination against the victims in order to spare his client's a conviction.

28 Just as the victims of sexual predators did not seek the rape, coercion or harassment or the *thrill*, nor did the victims of scammers. They were deceived in the strictest definition of criminal law in any EU jurisdiction. The victims were as trustful as they could be – and were assassinated and defrauded.

29 EFRI will do the best to give victims of scams and cybercrime a strong voice to protect them from being discriminated against and victimized again before the courts. We feel that victims left on their own are helpless in this cross-jurisdictional cybersociety. They have little to no hope of justice finally being served. It is time now to care about all this victims on the route of digitalization to stop people from ripping off innocent EU-consumers, and ashaming them.

30 We truly think it is long overdue that the European authorities take responsibility for all these victims and to unite in supporting us in our fight against these cybercriminals.

Your Sincerely

Elfriede Sixt Nigel Kimberly