BEFORE THE EUROPEAN UNION COMMISSIONER FOR JUSTICE, CONSUMERS, & GENDER EQUALITY

B E T W E E N:

CRYPTOCURRENCY VICTIMS

Claimants

-and-

BITCOIN VOLUNTARY ASSOCIATIONS, SOCIAL MEDIA, DOMAIN PRIVACY PROVIDERS, ET AL

Defendants

To: Commissioner Věra Jourová

From: Dr. Jonathan Levy, Solicitor and Attorney for Cryptocurrency Victims

In Re: Cryptocurrency Victim Claims - A Request for Consultation and Remediation

Reply by Victims to the Directorate's Response

We hereby respond to the Directorates' Reply of July 9, 2019 by Raluca Alexandra Prună and also supply further data to bolster our position.

1. The Commission has indicated as of January 10, 2020 it will begin to regulate crypto currency wallets and transactions on the national level.

We reply that this does not address any of the issues raised regarding past, ongoing and current losses by victims of crypto currency criminals or the transfer of billions of Euros to organized crime groups. Regulation of crypto currency wallets may prevent future money laundering and crime, but this provides no remedy or restitution for the tens of thousands of victims who have already lost billion of Euros to criminals. Regulation of wallets is not regulation of the voluntary associations known as crypto currencies and their ledgers. We respectfully point out that we seek a remedy for past wrongs that cannot be addressed without EU intervention. Regulation of wallets does absolutely nothing for existing victims of crypto crimes except to tacitly allows the criminals toe scape with billions of Euros.

2. The Commissions claims falsely that national courts provide a remedy.

If the Commission claims it lacks competence to deal with crypto crimes, how could national courts possess this ability? Most victims are destitute and unable to afford legal counsel to chase criminals whose identities have been shielded through the use of crypto currencies, identity theft, bitblending, and domain privacy providers. We have pointed out that the remedy lies with compensation from crypto currency (voluntary associations) ledgers, social media, and domain privacy providers who have obscenely profited at the expense of victims.

3. **The governments of several EU member states have created safe havens for crypto criminals.**

While the United Kingdom is not alone in creating cozy safe havens for crypto criminals, the position of the United Kingdom is likely the most egregious. The UK FCA has indicated it refuses to regulate crypt currency or address crypto crimes and swindles. The English Companies House is rife with fraud and false companies set up to provide cover for swindlers and the UK Foreign and Commonwealth Office actually allows the TLD .io to be used commit crimes with impunity. This violates current European Union AML and GDPR regimes and is within the competence of the Commission to investigate and take action upon.

4. The following supplemental information and claims are also submitted for your consideration:

I. The Position of the United Kingdom

We indicate in our initial submission that the government of the United Kingdom was remiss in its duties as to EU Anti Money Laundering and Data Protection regimes but was also fostering and actually aiding crypto currency crime and victimization by permitting unfettered access to its Companies House and TLD .io.

In fact, the situation is now critical.

We have made UK Freedom of Information requests seeking crypto currency crime data i.e.

Aggregate numbers of complaints and not identifying information for these categories:

- crypto currencies, Bitcoin, Ethereum etc.;
- initial coin or token offerings crypto currencies;
- other complaints in which crypto currencies were a factor.

These requests were made by this office and the replies indicates a complete pattern of disregard and indifference by UK authorities as to this issue:

UK Financial Ombudsman Service:

> As stated by the FCA on their website Exchange tokens (such as Bitcoin and 'cryptocurrency' equivalents) are not currently regulated in the UK. This means that the transfer, purchase and sale of

> exchange tokens, including the operation of exchange token exchanges, all currently fall outside the Financial Ombudsman Service remit and cannot be investigated.[1]

UK Financial Conduct Authority:

> Turning now to your request, as explained above we do not deal with general complaints and therefore do not hold a central record whereby an expression of dissatisfaction may have been received. Whilst our Customer Contact Centre (CCC) retains a record of all contacts, it will be difficult for us to locate an accurate number for how many of those contacts contain an expression of dissatisfaction without undertaking extensive searches.[2]

UK Metropolitan Police Service

> To locate the information relevant to your request searches were conducted with the Organised Crime Command, responsible for investigating cybercrime, and the Performance and Assurance Unit, responsible for extracting corporate statistics. Unfortunately, this email is to inform you that it has been confirmed by both units that it will not be possible to respond to your request within the cost threshold.[3]

UK National Fraud Authority:

> The National Fraud Authority (NFA) ceased to exist in March of 2014. No single body took over its remit.[4]

UK Information Commissioner's Office:

> While it is likely that we hold information in scope of your request, unfortunately we are not able to provide you with the information you have requested.[5]

---

[1] Full details of request available at:
https://www.whatdotheyknow.com/request/statistics_for_complaints_regard#incoming-1381313
[2] Full details of request available at:
https://www.whatdotheyknow.com/request/crypto_currency_complaint#incoming-1380491
[3] Full details of request available at:
https://www.whatdotheyknow.com/request/crypto_currencies_3#incoming-1378153
[4] Full details of request available at:
https://www.whatdotheyknow.com/request/crypto_currencies#incoming-1374320
[5] Full details of request available at:
https://www.whatdotheyknow.com/request/crypto_currency_related_complain_2#incoming-1372374

UK Serious Fraud Office:

> We received 10 referrals during 2018 that involved cryptocurrencies. However, I can neither confirm nor deny whether any criminal investigations involving the misuse of cryptocurrencies were opened during that year.[6]

Based on this sample one can draw the conclusion that the UK does not take crypto currency related crime seriously and in fact is attempting to obfuscate the issue to cover up their misfeasance under EU data protection and AML regimes. For all intents and purposes the United Kingdom government is welcoming criminals and organized crime to use the .io TLD and Companies House Registry to further their unlawful schemes. In addition the UK FCA by enacting a public "hands off" policy towards crypto criminals and their schemes, has declared the United Kingdom is "open for business;" the business of crypto criminality and money laundering.

II. The Position of the European Union

It must be noted that the UK is not the only entity that refuses to answer these crypto currency crime related requests for data, the European Police Office is similarly remiss. A May 9, 2019 request along the same lines has not even been acknowledged by the European Police Office and an internal review request has been filed.[7]

III. Bitmixing

We note that despite media reports that EUROPOL has been active regarding interdiction of Bitmixing i.e. money laundering of crypto currency that the Bitcoin Blender Organization consisting of bitblender.io and its sister site bitblender.co remain active despite being under the jurisdiction of the British Indian Ocean Territory Administration and UK Foreign and Commonwealth Office. We fail to understand how criminal money laundering enterprises are permitted to operate from the .io TLD (Top level Domain) controlled by the UK Foreign and Commonwealth Office contractors BATELCO/SURE (Camp Justice, Diego Garcia, British Indian Ocean Territory) and Internet Computer Bureau (UK) especially when the British Indian Ocean Territory are constitutionally declared a sort of restricted military zone:

> No right of abode in the Territory
> British Indian Ocean Territory Constitution Order 2004

[6] Full details of request available at:
https://www.whatdotheyknow.com/request/crypto_currencies_2#incoming-1370080
[7] Full details of request available at:
https://www.asktheeu.org/en/request/crypto_currency_related_complain#outgoing-13877

> 9. — (1) Whereas the Territory was constituted and is set aside to be available for the defence purposes of the Government of the United Kingdom and the Government of the United States of America, no person has the right of abode in the Territory.
>
> (2) Accordingly, no person is entitled to enter or be present in the Territory except as authorised by or under this Order or any other law for the time being in force in the Territory.[8]

The lack of interest by the UK government is no doubt behind Bitblender (Bitcoin Blender Organization) becoming so emboldened that it has opened a sister site bitblender.co to solicit further business for its dark web money laundering for hacked, extorted and illegally obtained crypto currency.

IV. Additional Victim Claims and Statements

Mr. BN is a resident and citizen of the United Kingdom. He maintained an Instagram page wherein some of the content indicated an interest in crypto currency investment. He was approached by a tout using the Instagram messaging tool offering him a professionally managed investment account. The tout's account indicated tens of thousands of followers which provided some indicia of legitimacy. The WhatsApp messaging tool was also utilized to open an account with globalcoinhash.com. Globalcoinhash.com purports to be in the United Kingdom: "We have a Mining Farm ring that produces 3000 bitcoins daily using SHA 256 Algorithm specialised hardware and we also trade forex binary and cryptocurrency with an auto trade software the guarantees 100% Profit Return." In fact, it is a criminal organization using a cloaked website registered to WhoisGuard, Inc. of Panama City, Panama. Through the use of false accounting BN was induced to invest $24,000, a portion of which were fraudulent taxes and fees levied by globalcoinhash.com. When BN's balance reached $124,000, the criminals then demanded an advance fee which BN refused to pay, BN's losses include identity theft and exceed $100,000 in out of pocket losses, lost profits, and damages.

HLH is citizen and resident of Namibia. He invested in Bitcoin and became interested in mining Bitcoin after he read about it on social media. He was approached by a tout via social media (LINE) who induced him to invest over $200,000 in what HLH believed to be a legitimate Bitcoin mining platform, playcoin11.com. The ownership of playcoin11.com is unknown, its website used a proxy registrant, Domains By Proxy, LLC, based in the United States. HLH was provided false accountings that showed his account balance exceeded $1 million. However, by June 19, 2019, the entire purported mining operation vanished from the Internet along with his investment. HLH's identity documents were also compromised by playcoin11. HLH seeks his investment and lost profit totaling at least $1 million.

[8] British Indian Ocean Territory Constitution Order 2004
https://en.wikisource.org/wiki/British_Indian_Ocean_Territory_Constitution_Order_2004

Lucien C. is a resident of the United States. In May 2019 as a result of social media postings and messages (WhatsApp, Instagram, LinkedIn) and a referral he invested Bitcoin crypto currency in what he thought was a legitimate trading platform, Iqtradechain.com. Iqtradechain claims to operate offices in the USA, Belgium and England. He was provided numerous false accountings, so he would invest further crypto currency. When he tried to withdraw so called profits, he was advised he had to pay advance fees at which he realized this was a criminal operation intent only on extorting further funds. The criminals also obtained his identity documents under false pretenses. His damages exceed $50,000.

S srl** is an Italian company. The other co-claimants, **RA, PF, and AT** reside in Italy and invested jointly with S** and are citizens of Italy. They all invested funds in AXECC.IO (AXE Crypto Currency or AXECC) which purports to be a crypto currency trading or investment platform with no fixed abode or office except for its Top-Level Domain .io website: axecc.io. The domain registration for axecc.io is masked and leads to a privacy service Whois Privacy Corp. in Nassau, The Bahamas which is listed as the domain registrant. AXECC through its network of brokers and/or touts induced Claimants using social media like WhatsApp to deposit at least €260,000 in a series of transactions from January 2018 through February 2019, the majority of which were obtained through the simple expedient of providing a running false accounting showing trading profits. Claimants' payments were made to AXECC in a series of transactions. Some of the payments were for arbitrary assessments by AXECC such as "insurance," "taxes" and "fees." The payments were in mixed transactions of currency and crypto currency. Claimant also provided identity documents to AXECC. Losses include £242,000 in various currencies and crypto currencies and damages for lost profits and identity theft. Claimant seeks €1.2 million in compensation.

Mr. GC is a citizen of Spain. Being interested in investing in crypto currency he enrolled in several crypto currency related Telegram social media groups not knowing these were essentially hunting grounds for criminals. He was a multiple victim. Beginning in March 2019, he invested over $10,000 through the now defunct website bitshell.io which also used the Companies House registration for Bitshell Ltd. to provide legitimacy. Both were shams and simply provided false accountings and ultimately disappeared with GC's funds and $10,000 in profits. The .io domain bitshell.io is registered to "Privacy Guardian" whose website states: All mail addressed to our PO Box or our email address will be discarded without looking at it. GC at the same time also invested in a similar criminal enterprise bitlemon.net which is also defunct, his losses totaled approximately $10,000 in deposits and lost profits. Additionally, he invested in another scheme bitcabinet.biz with similar circumstances and results for losses totaling $4000 in deposits. Bitcabinet.biz is also defunct and utilized a dissolved Companies House shell, Bitcabinet Group Limited, to provide a façade of legitimacy. GC also lost over €15,000 in the now defunct unlicensed trading platform bluetrading.com which utilized and traded in crypto currency. Blue Trading was purportedly the product of Russian organized crime. GC seeks over €50,000 in damages and losses including identity theft.

V. Domain Privacy Providers

We continue to see the use of Domain Privacy Providers to completely shield the one clue to the crypto criminals' identity, their domain registrations. The Domain Privacy Providers are well aware their client are criminals – HYIP Ponzi Schemes, unlicensed FOREX and Crypto traders, and other fraudulent schemes. For example, bitblender.co uses US based Privacy Protect, LLC. Privacy Protect, LLC is part of a much larger organization which purports to have AML procedures in place, yet a bitmixing or bitblending operation is *de facto* money laundering and could never be a legitimate enterprise. Internet Computer Bureau, the sub administrator of the .io domain has gone even further by disabling the registrant data in its nic.io database for many of these operations and making it difficult even to locate the Domain Privacy Providers. Measures must be taken against Domain Privacy Providers who knowing shield criminal operations.

VI. Social Media

Social media also continues to be a contributor to the crypto crime problem. Facebook, Telegram, Instagram, and WhatsApp in particular generate vast amounts of leads for the crypto criminals. Ponzi type schemes are easily identifiable using even rudimentary artificial intelligence programs, yet we are seeing no overall attempt to interdict or police.

VII. Crypto Currencies

Crypto currencies have generated vast wealth for their users and promoters yet have contributed not a single penny towards indemnifying victims. The recent "bull market" which has seen 100% gains has not benefited victims. This unbridled greed and opportunism must be regulated and victims compensated. The fraudulent Nakamoto and similar proxy ledger entries should be seized to reimburse victims.

VII. Conclusion

We are requesting the Commission reassess its position and address the transfer of billions of Euros of assets into the hands or organized crime at the expense of victims. We also are requesting the Commission independently investigate the consumer related aspects of our Request including but not limited to the roles of false entries on the crypto currency (voluntary association) ledgers such as the "Nakamoto coins," bitblending, The English Companies House, domain privacy providers, social media and the TLD .io.

Respectfully Submitted,

Dr. Jonathan Levy[9]
Attorney & Solicitor
Legal Representative for Crypto Currency Victims

[9] Dr. Jonathan Levy is a licensed attorney and European lawyer (Ireland). He holds a PhD in Political Science as is a faculty member at Norwich University and a member of the Institute for National and International Security (INIS). For English law matters, he is a consulting solicitor at the firm of Berlad Graham LLP.