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

Date: September 23, 2019

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

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

Supplementary Reply by Victims to the Directorate's Response

We hereby tender our supplementary response to the Directorates' Reply of July 9, 2019 authored by Raluca Alexandra Prună.

We incorporate by reference:

Cryptocurrency Victims Communications of June and July 2019 and the Commission's Reply of July 2019.

1. The Commission has not yet responded to our follow up Communication of July 9, 2019.

On or about July 9, 2019, Cryptocurrency victims replied via electronic mail to Commissioner Jourová and Ms. Prună. No reply to our July 9 communication (attached) has been received.

2. The Commission has not made Anti Money Laundering reports.

The Commission has apparently failed to act or report the criminal organizations highlighted in the previous two communications even though it has a general duty to do so. This amounts to nonfeasance and permit criminals to operate with impunity and without fear of detection within the EU even when their activities are reported at the highest levels.

These criminal organization continue to operate unhindered by EU or national authorities including:

Bitblender.io

Doubly

Etherdelta.com

FinTech Mining

Zilton Capital

CryptoAllDay

MGM Markets

CCT Market

Global Coinhash

National courts are not equipped to handle cryptocurrency victim claims. This is proven by the lack of viable remedies in any of the EU member nations. This complete lack of remedy has led many cryptocurrency victims in desperation to be cheated yet again by criminals using social media who falsely claim they can retrieve the victims' funds from "the blockchain" in exchange for an advance fee.

3. **The impending Brexit further complicates the situation of victims.**

Many crypto criminal operations may be traced to the United Kingdom. Without strong protections in place; these victims' claims will be lost as the United Kingdom withdraws from the European Union and its consumer and data protection regimes**.** As noted *infra*, the United Kingdom position is that cryptocurrency is an unregulated entity; this we believe violates common EU rules on data protection, anti-money laundering and payment processing.

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

I. The Position of the United Kingdom

The position of the United Kingdom is perhaps the most problematic from the standpoint of cryptocurrency victims.

On July 31, 2019, the United Kingdom Financial Conduct Authority (FCA) published its "Guidance on Cryptoassets.[1]" The vast majority of cryptoassets which the FCA classified as

[1] Available at https://www.fca.org.uk/publication/policy/ps19-22.pdf

exchange tokens and their derivatives - including Bitcoin and Ethereum - were found to be outside the remit of the FCA, accordingly denying victims any meaningful access to assistance with their claims against crypto criminals.

Additionally, the UK Foreign and Commonwealth Office ('FCO') continues to deflect any attempts to penetrate the .IO top level domain, which is subject to a secret agreement between the FCO and an English company, Internet Computer Bureau and its parent company, the Irish private firm, Afilias Limited which in turn is a subsidiary of the US firm, Afilias Inc. Time and time again .IO based crypto scams and criminal organizations have been undisturbed by British law enforcement. The City of London Police, which has jurisdiction over some forms of economic fraud in the United Kingdom, has reported an additional 230 instances of alleged fraud regarding .IO sites in 2018 down slightly from 328 reports in 2017; there is no suggestion any of these reports led to prosecution.[2] [3] The control of the lucrative .IO domain is further complicated by the Diego Garcia dispute; both the International Court of Justice and United Nations General Assembly have taken the position that the UK should vacate British Indian Ocean Territory, which would include the .IO Domain Registry and Internet Administrator both of which are nominally based on Diego Garcia Island according to the IANA (Internet Assigned Number Authority) Delegation Record for .IO.[4]

II. The Position of the European Union

The European Police Office (EUROPOL) has refused to respond to two requests by Cryptocurrency Victims' counsel under EU Regulation 1049/2001.

The first request made May 9, 2019 seeks the aggregate numbers of complaints and not identifying information for these categories: crypto currencies (Bitcoin, Ethereum etc.), complaints about initial coin or token offerings crypto currencies and other complaints in which crypto currencies were a factor. EUROPOL has refused to acknowledge the request or a follow up request for initial review.[5]

A second request made on June 26, 2019 to EUROPOL seeks all available information on Bitmixing, Bitumbling, or Bitblending, which is the laundering of Bitcoins through services like Bitmixer and Bitblender but not limited to them. EUROPOL has also refused to acknowledge or respond to this request.[6]

As noted above, Cryptocurrency victims are also concerned that the EU Commission itself is ignoring its own rules on anti-money laundering. Not only are the criminal organizations listed *supra* still in operation cheating and swindling victims, but bitmixing which the EU

[2] See: https://www.whatdotheyknow.com/request/547012/response/1411533/attach/html/4/FOI%20COL%2019%20120.docx.html
[3] See: https://www.whatdotheyknow.com/request/488184/response/1178812/attach/html/3/18%20506.pdf.html
[4] See: https://www.iana.org/domains/root/db/io.html
[5] See: https://www.asktheeu.org/en/request/crypto_currency_related_complain#outgoing-13877
[6] See: https://www.asktheeu.org/en/request/bitmixing#outgoing-14153

admits is money laundering *per se* continues to be virtually based in an EU member's (United Kingdom) overseas territory, the British Indian Ocean Territory – see Bitmixing *infra.*

If counsel is unable to elicit even a basic response from EUROPOL and the EU Commission cannot be bothered to make AML reports, what hope do cryptocurrency victims have under the current EU policy?

III. Bitmixing

National authorities continue to ignore the laundering of cryptocurrency by criminals using bitmixers and bitblenders which render the cryptocurrencies untraceable.

Cryptovictims' counsel was able to effect the closure of the notorious site bitblender.co through legal means, though no recovery of victim assets was possible. Despite ongoing legal process in the British Indian Ocean Territory Supreme Court, bitblender.io and its progeny mixers including smartmix.io, smartmixer.io, cryptomixer.io, anonymix.io, blender.io, mixtum.io, privcoin.io, mixm.io, and others continue to operate without interference. The UK FCO by its lack of oversight of the .IO domain is facilitating money laundering on a grand scale: billions of Euros over the past three years, of which it has been repeatedly apprized.

This constitutes a flagrant violation of EU AML treaties and rules by an EU member state.

IV. Crypto Mining (Reserved)

It has long been suspected that many crypto mining ventures, particularly those like AWS Mining (see claim by DC below) which allegedly operated mines in out of the way places like Paraguay, Russia, and China, were in fact criminal pyramid schemes. EU residents have been victimized by crypto mining scams and cloud mining scams to a large degree. Consumer protection from these frauds is complicated by their multi-jurisdictional nature. We expect significant claims to develop in this area and as such compensation should be reserved for victims where cryptocurrency was both the object and means of the criminal behavior.

V. ICOs - Initial Coin or Token Offerings (Reserved)

A substantial claim involving TRIG coin or token is detailed *infra.* TRIG is typical of hundreds if not thousands of so called ICO coins or tokens. For the most part, these coins are worthless and were vehicles for organized crime pump and dump schemes. The criminal element that formerly utilized penny stocks, boiler rooms, and binary FOREX moved over to cryptocurrency based ICOs with disastrous consequences for victims. High pressure sales tactics were unleashed on cryptocurrency victims. Various crypto exchanges facilitated this criminal avalanche by listing ICOs with little or no oversight. A website, social media presence, and a so-called whitepaper were usually the only requirements for an ICO. We expect significant claims to develop in this area and as such compensation should be reserved for victims where cryptocurrency was both the object and means of the criminal behavior.

VI. Online Casinos (Reserved)

Cryptocurrency Victims' counsel have been in touch with EU resident victims of cryptocurrency-based casinos. It is highly likely that erstwhile gamblers using online cryptocurrency-based casinos have been defrauded of hundreds of millions of Euros by unlicensed gambling operations operated by organized crime syndicates. The criminals often process payments through banks and financial service providers in Cyprus and Malta. We expect significant claims to develop in this area and as such compensation should be reserved for victims where crypto currency was both the object and means of the criminal behavior.

VII. Bank Fraud

Claimant VG below details the use of an unlicensed Internet bank (Sun Financial Bank) to process victim payments and or to defraud victims. Additionally, claimant S** srl from our communication of July 2019, reports that affiliates of the criminal organization AXECC.IO have recently attempted to utilize forged Barclays Bank indicia to further defraud the victim. In each case, national authorities and banks who were the subject of impersonation were notified. In each case no action was initiated by national authorities (California and UK) nor were the complaints acknowledged by the banks (Sun Trust and Barclays) impersonated. The lack of action is directly related to the ambiguous position of national authorities regarding cryptocurrency. Victims therefore have no remedy and criminals may operate with impunity in violation of basic anti money laundering and banking fraud rules.

VIII. Additional Victim Claims and Statements

IB is a resident and citizen of the United States and was an investor in crypto currency. In May 2019 he was contacted on the telephone by a representative of STSCrypto or STSCrypto.com. STSCrypto falsely claims to be a crypto currency trading platform owned and operated by a private German shell company: Capital Letter GmbH, Registration Number HRB242418, Adolf-Kolping-Straße 16, 80336 München, Germany. STSCrypto is in fact a criminal organization set up to defraud and extort crypto currency from individuals. The call screener discovered IB was interested about investing in crypto currency and quickly put IB in touch with a professional tout working for STSCrypto. The tout promised IB profits and by means of false accountings induced him to transfer over €110,000 in crypto currency from his Coinbase account. When the account showed a balance of approximately €140,000, IB was subjected to a high-pressure pitch to upgrade the account and pay various fees. Based on these misrepresentations, IB paid €10,000 in fraudulent fees. In an attempt to extort even more money, the criminals at STSCrypto provided false blockchain transaction hash codes to IB when he unsuccessfully attempted to withdraw funds. IB seeks compensation of €150,000 for his direct losses involving crypto currency.

SS is a citizen of India. In 2016 she was approached by a third party who induced her to invest $500 worth of Bitcoin in a venture. The investment and the Bitcoin simply disappeared with no way to trace the investment or payment due to the nature of Bitcoin and its blockchain.

The current value of the Bitcoin invested is no less than €10,000 which is the amount of compensation sought from the Bitcoin Voluntary Associations.

VG is a citizen and resident of Kosovo. In 2018 Mr. VG was induced by a criminal posing as an American financial advisor utilizing a stolen copy of a US passport and false Instagram, LinkedIn, and Facebook accounts to invest approximately €45,000 in crypto currency with a fraudulent trading platform called 21st Options in a series of transactions based on false accountings showing massive profits. 21st Options or 21stoptions.com purports to have offices in California, Texas and Luxembourg utilizing a variety of phone numbers and addresses based in the US, UK, Germany and Luxembourg. 21st Options claims: "Our HQ is in Gde-Duchesse Charlotte, Luxembourg, and we're licensed by the CSSF. With us you can trade over 400 forex and CFD financial instruments, including currency pairs, shares of your favourite companies, crypto currencies, popular commodities and indices from around the world. All trades are done using forex or contract for difference." However, 21st Options is not licensed by the Luxembourg Commission de Surveillance du Secteur Financier (CSSF) and is a purely criminal organization. When VG's account showed a total of over €750,000 in principal and profit, he sought to make a withdrawal. In a complex series of attempts throughout 2018-2019, 21st Options demanded an advance payment fee of over €100,000 from VG. When VG refused to pay, the criminals attempted to extort the funds by claiming the account would be donated to UNESCO due to violations of United States securities laws and International Monetary Fund rules. 21st Options also attempted to persuade VG to deposit funds at a false banking platform, Sun Financial Bank, https://sunfinportal.com. VG reported these transgressions to numerous national authorities with no results. He seeks return of his funds, lost profits, and damages for emotional distress in the amount of €300,000.

DC is a Romanian resident and citizen who represents a group of 13 Romanian investors or victims in the Australian based criminal organization AWS Mining Pty Ltd. or awsmining.com. AWS Mining purports to be a crypto currency mining operation with operations in remote locations in Russia, Paraguay, and China. It is unlikely any of these so-called mines exist as crypto currency mining is unlawful in China and Russia and AWS is in reality a criminal pyramid scheme. AWS Mining utilized crypto currency both as the bait and means of its criminal operations. The Romanian victims invested at least €100,000 between August 2018 and August 2019 on promises that their funds would double in 12 months. The criminals utilized MLM (Multi-Level Marketing) tactics and a Telegram group in furtherance of the scheme. In April 2019 the victims were falsely told there was a fire and their mining machines were damaged in an attempt by the AWS crime firm to extort further funds. The DC group seeks a refund of their crypto currency and lost profits totaling €200,000.

David H is a citizen and resident of the United Kingdom as previously noted in our Communication of June 3, 2019. In addition to his losses to a criminal crypto trading platform, he has since lost €500,000 on a failed and fraudulent crypto coin or token called Blocksafe Trigger or TRIG which traded on the world's leading cryptocurrency exchange Binance which conducts business in Malta and Jersey. Binance failed to self-regulate or validate TRIG which

conducted a successful pump and dump (P&D) operation netting tens of millions of Euros from investors like David H in exchange for its worthless cryptocurrency-based coins or tokens. Only after the successful sale of it coins or tokens to unwary investors did Binance delist TRIG. Likewise, TRIG was also promoted and sold on the United States based Bittrex Exchange. David H acquired his TRIG on both Binance and Bittrex. TRIG appears to have operated from the United States or Puerto Rico and made the preposterous claim that its purpose was to develop sensor-based defense technologies by offering a robust network capable of hosting innovative solutions. The coin's promoters also claimed: "They will be meeting with the Air Force, filing patents, and attending various summits in the coming months. The company announced that its intellectual property holding partner is planning to go public in both Canada and the United States through a traditional stock offering." In fact, TRIG was delisted from most exchanges, and tried to fold the venture leaving the investors with nothing. David H. seeks compensation of €500,000.

PM is a citizen and resident of the United States. Beginning in January 2019, he invested 10 BTC (Bitcoins) worth approximately €100,000 with an organization called Profitcoins or profitcoins.io. Profitcoins claimed by using arbitrage trading it could increase a depositor's Bitcoins. When PM's deposit grew to 30 BTC (Bitcoins), he attempted to make a withdrawal. He repeatedly tried to make a withdrawal but never received anything because Profitcoins was a criminal organization that utilized Bitcoin and false accounting to commit theft. Profitcoins like many other crypto criminal firms utilizes and continues to utilize the .IO domain owing to no enforcement of Anti Money Laundering rules by the UK FCO and has registered a shell company with the UK Companies House called Profitcoins Ltd. in order to provide a façade of legitimacy. PM also invested 30 BTC (Bitcoins) with a so-called crypto cloud mining operation called Teslminer in 2017. The deposit value grew to an estimated 60BTC before Teslaminer and its deposits disappeared with no trace. PM seeks compensation of no less than €500,000.

IX. Social Media

Social media also continues to be a contributor to the crypto crime problem. Telegram groups in particular continue to be utilized by crypto criminals to defraud investors as in the case of Doubly.io and others mentioned herein.

X. Bitcoin

The Bitcoin Voluntary Associations through their "full nodes" continue to operate in the European Union as unlicensed payment services in violation of EU rules on Payment Services and Anti Money Laundering. The full nodes also act as unlicensed transfer agents in relation to the Bitcoin ledger. Bitcoin full nodes are required to charge a default Minimum Relay Fee of .0005 Satoshi per transaction as determined by the Bitcoin Voluntary Associations. Some full nodes however charge more. .Bitcoin 24-hour volume processed by the Full Nodes of the Bitcoin Voluntary Association continues at a rate of at least € 10 billion. This is highly

indicative of a unified scheme by the Bitcoin Voluntary Associations making them subject to EU regulation as payment services and subject to AML and GDPR rules.

5. Conclusion

Cryptocurrency Victims are requesting the Commission substantively address the concerns raised by the Cryptocurrency Victims and immediately enter into consultations regarding the funding of a Cryptocurrency Victims Fund to be financed initially from the Nakamoto coins fraudulently entered on the Bitcoin Voluntary Associations ledger and supplemented from other sources including fees on daily transactions in cryptocurrency. Additionally, the Commission is reminded that no organization is above the law and that nonfeasance of crypto crime is never an answer. Finally, given the prevalence of crypto criminality in the United Kingdom, the attitude of nonregulation and inexplicable aiding and abetting of crypto criminals by the British Crown. Cryptocurrency Victims will escalate this matter to a more formal legal procedure before the Brexit date of October 31, 2019 unless significant progress is made by that time.

Respectfully Submitted,

Dr. Jonathan Levy[7]
Attorney & Solicitor
Legal Representative for Crypto Currency Victims

[7] 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.