European Ombudsman

Search...

MAKE A COMPLAINT

Complaint about maladministration

Complaint submitted on: Sunday | 01 December 2019

European Ombudsman

First name:	Jonathan
Surname:	Levy
Address line 1:	Unit 7810
Address line 2:	PO Box 6945
Town/City:	London
County/State/Province:	
Postcode:	W1A 6US

Country:	United Kingdom
Nationality	American/of the United States
Tel.:	+44 (0) 20 8144 2479
E-mail address:	info@jlevy.co
Language preference	English
On behalf of (if applicable):	Association/Organisation/NGO
E-mail address:	
Entity Name	National Liberal Party and Cryptocurrency Victims
Address line 1:	PO Box 4217
Address line 2:	
Town/City:	Hornchurch
County/State/Province:	Essex
Postcode:	RM12 4PJ
Country:	United Kingdom

Against which European Union (EU) institution or body do you wish to complain?

European Commission

What is the decision or matter about which you complain? When did you become aware of it? Add annexes if necessary.

Petitioners (the National Liberal Party (UK) and the Cryptocurrency Victims) are represented by their legal counsel Dr. Jonathan Levy. Petitioners both citizens of the European Union and non-citizens who have been harmed by events within the European Union involving cryptocurrency. Petitioners' fiscal losses, legal fees and costs and damages exceed €28,000,000. See Exhibit 1 identifying petitioners and their losses including Power of Attorney for new petitioners who are joining this action. Petitioners were all victims of cryptocurrency criminals including Ponzi schemes, hackers, unlicensed and or unlawfully operating Internet casinos, "bitmixers," Initial Coin Offerings, identity and data theft, forgery and unlicensed Internet brokers.

Petitioners and their legal counsel attempted to resolve their losses by initiating a variety of measures including civil legal process in national

courts, criminal complaints to national authorities, bank wire and credit card reversals, blockchain tracing and other legal demands upon criminals, exchanges, domain privacy providers, domain registrars, national governments and cryptocurrencies. None of these remedies were successful owing to the multijurisdictional nature of cryptocurrency transaction, the anonymity afforded therefrom, Internet domain ownership shielded by uncooperative third party privacy providers, incomplete Internet domain registration information, false identities, uncooperative banking authorities, law enforcement agency unwillingness to open criminal cases, lack of national judicial jurisdiction, and overall unwillingness by national authorities to police or regulate cryptocurrency and crimes and related money laundering, unlicensed money transfers, or prevent their country code top-level domain (ccTLD) from being utilized by criminals operating openly and notoriously.

Several jurisdictions such as Russia and China have realized that cryptocurrency and its upwards of €100 billion daily volume cannot be adequately regulated under their laws and have banned such activity. Much of the cryptocurrency criminal activity originates from the EU or uses the EU banking system. In particular United Kingdom shell companies, Bulgarian and Cypriot bank accounts and payment processors, UK and EU controlled ccTLDs, and EU based exchanges and crypto currency nodes are favored or utilized by the criminals. In addition, a large number of cryptocurrency victims are concentrated within the EU due to lack of regulation and nonenforcement of national laws to cryptocurrency crimes in countries like the United Kingdom, Latvia, Estonia, and Bulgaria.

On April 22, 2019, Cryptocurrency Victims' legal counsel make a request for access to documents, registered on April 24, 2019 under reference number 2019/13 to the European Union Data Protection Board (EDPD) in order to access: "(A)ll working papers and other information that address the GDPR and its application to Bitcoin and other crypto currencies. " The purpose of the request was to determine whether the European Union had taken jurisdiction over cryptocurrencies under the GPDR or some other EU wide regime as cryptocurrency by definition is data transmitted over a "blockchain."

On May 17, 2018 the Vice Chair of the EDPD replied and noted that the EDPD was addressing the issue as well as other EU agencies, notably the

European Parliament were in the process of addressing cryptocurrency under not only the GDPR but other regulatory schemes. See Exhibit 2.

Having affirmed the EU was indeed addressing a cryptocurrency regulatory or enforcement regime under the GDPR and other rules, Cryptocurrency Victims' legal counsel then sent a "Request for Consultation and Remediation" on June 3, 2019 to the European Commission, Ms. Vera Jourová, Commissioner for Justice, Consumers and Gender Equality. See Exhibit 3. This request stated in detail the grounds upon which the Cryptocurrency Victims requested the European Commission to take up the matter of cryptocurrency crime victims under both the General Data Protection Rules (GDPR), EU Anti Money Laundering laws and general notions of justice. The remedies suggested involved creating a fund for cryptocurrency victims from the "Nakamoto" assets on the ledgers of unincorporated entities known as decentralized permissionless cryptocurrencies and by holding social media and domain privacy and proxy services financially responsible for cryptocurrency crimes utilizing their platforms and services.

On July 9, 2019, Ms. Raluca Alexandra Prună, Head of Unit, Directorate General Justice and Consumers, Directorate B – Criminal Justice responded on behalf of the Commission to the Letter of June 3, 2019. See Exhibit 4. Ms. Prună selectively admitted that the Commission did have jurisdiction over cryptocurrency in that:

1. EU Anti Money Laundering rules applied to cryptocurrencies via Directive (EU) 2018/843.

2. FATF anti money laundering rules also generally applied to cryptocurrencies

The Commission however refused to take up the concerns of Cryptocurrency Victims because:

" (T)he Commission does not have the competence to address such individual problems, which remain in the hands of national courts, to which we suggest you to revert."

On July 10, 2019, Cryptocurrency Victims through their legal counsel Dr.

Jonathan Levy responded to the Commission and raised additional cases and concerns as follows. See Exhibit 5.

1. National courts were failing to provide a remedy for victims of cryptocurrency crimes.

2. The United Kingdom in particular was deliberately providing a safe haven for crypto criminals though its hands-off policy on crypto crime and continued promotion of the ccTLD .IO for use by crypto criminals.

3. EUROPOL and national authorities were failing to address the issue of "bitmixing" which by the EU's own definition was money laundering per se.

Cryptocurrency Victims reiterated their request of the Commission as follows:

"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," bitmixing, The English Companies House, domain privacy providers, social media and the TLD .io."

On September 23, 2019, Cryptocurrency Victims through their legal counsel Dr. Jonathan Levy made another request to the Commission. See Exhibit 6. This request raised additional cases and concerns as follows:

1. The Commission having been apprised of specific and significant cryptocurrency criminal activity by the Victims had failed to take any action as the criminals continued to operate unimpeded.

2. The United Kingdom government's cryptocurrency policies continued to be problematic and its policies were frustrating victims attempts to obtain justice.

3. Billions of Euros continued to be transferred from victims to organized crime due to the Commission's failure to act against criminal operations including: online casinos, "bitmixers," ICOs (Initial Coin offerings), crypto mining, and bank fraud.

Victims also pointed out that Bitcoin itself was far from being a decentralized permissionless non entity but in fact was a juridical person under EU jurisdiction:

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

On October 21, 2019, the Commission responded to Cryptocurrency Victims' legal counsel Dr. Jonathan Levy. See Exhibit 7. The Commission noted receiving the previous two communication from Cryptocurrency Victims and again stressed its Anti Money Laundering jurisdiction without commenting on the applicability of the GDPR or Payment Processing rules to cryptocurrency. The Commission stressed: "(T)he Commission has currently no competences on this issue and urge you once again to seek a remedy under your national judicial system."

What do you consider that the EU institution or body has done wrong?

The Commission has acknowledged that it's Anti Money Laundering rules apply to cryptocurrencies and related crimes. The Commission has acknowledged the seriousness of the situation. Yet, it refuses to take any actions that would assist tens of thousands of victims of multijurisdictional cryptocurrency crimes involving billions of Euros and the EU. The Commission has also refused to address other issues by omission including the applicability of its GDPR and Payment Processing rules to

cryptocurrency crimes.

This amounts to Maladministration in that only the Commission has accepted jurisdiction and should remedy the situation given the refusal of national courts and agencies to act on behalf of Victims.

The Commission's lack of action and nonfeasance in the face of billions of Euros lost annually to criminal activity, theft, fraud, money laundering, and with terrorist financing occurring everyday and touching the EU is extraordinary, inexplicable, arbitrary, and capricious.

What, in your view, should the institution or body do to put things right?

The Commission must act with all alacrity to:

1. To deploy existing anti money laundering, GDPR, and payment processing regimes to prevent further rampant criminality and exploitation of victims.

2. Create a remedy for Cryptocurrency Victims by establishing a funding mechanism from the Bitcoin Voluntary Association and other cryptocurrencies ledgers and relay fees, social media, and third party privacy providers and encourage these parties to settle claims.

3. Take action against the United Kingdom government so that it does not continue to provide a safe haven for crypto criminals.

4. The Commission must also follow its own rules on AML, GDPR, and payment processing regarding the ccTLD .EU. The EU domain is owned by the EU and operations delegated under contract by the Commission to EURid (European Registry for Internet Domains). Arguably, the most notorious cryptocurrency criminal organization is the One Life/One Coin operation. It is estimated to have stolen over €4 billion from victims including over €1,000,000 from Cryptocurrency Victims. See Exhibit One. One Life continues to operate despite criminal prosecutions in the United States, China, and elsewhere. One Life operates from Internet platform - https://www.onelife.eu

The EU Commission itself like the United Kingdom is actively aiding and abetting cryptocurrency criminals in violation of its own rules and laws in

the most notorious of all cryptocurrency criminal gangs is operating from the Commission own ccTLD without fear of prosecution or hindrance owing to malfeasance by the Commission.

Have you already contacted the EU institution or body concerned in order to obtain redress?

Yes (please specify and submit copies of the relevant correspondence)

Yes, see Exhibits. The Commission has refused reasonable requests to meet and confer on these issues or implement even modest measures to assist victims.

If the complaint concerns work relationships with the EU institutions and bodies: have you used all the possibilities for internal administrative requests and complaints provided for in the Staff Regulations? If so, have the time limits for replies by the institutions already expired?

Not applicable

Has the object of your complaint already been settled by a court or is it pending before a court?

Please confirm that you have read the information below

You have read the information note on data processing and confidentiality

Do you agree that your complaint may be passed on to another institution or body (European or national), if the European Ombudsman decides that he is not entitled to deal with it?

Yes

Attachments:

Name	Size
Exhibit 7 EC Response 10-19.pdf	119.1 KB
Exhibit 4 EC Response 7-19.pdf	157.05 KB
Exhibit 7 EC Response 10-19.pdf	119.1 KB
Exhibit 6 Reply 9-19.pdf	249.34 KB
Exhibit 5 Reply 7-19.pdf	206.57 KB
Exhibit 2 letter from EDPD.pdf	1.91 MB
Exhibit 3 Request to EC 6-19.pdf	265.17 KB
Exhibit 1 Table of Complainants.pdf	2.33 MB
Exhibit 6 Reply 9-19.pdf	249.34 KB
Exhibit 4 EC Response 7-19.pdf	157.05 KB
Exhibit 5 Reply 7-19.pdf	206.57 KB

Exhibit 3 Request to EC 6-19.pdf 265.17 KB

1, avenue du Président Robert Schuman
CS 30403
F - 67001 Strasbourg Cedex

T. +33 (0)3 88 17 23 13
F. +33 (0)3 88 17 90 62

www.ombudsman.europa.eu

Follow us