

**Data Protection Office**

Police Headquarters, Saunders Lane, Hutton, Preston PR4 5SB

Tel: 01772 413203 / 412144

Email: [FOI@lancashire.police.uk](mailto:FOI@lancashire.police.uk)



Rob Davies

Sent via email to: request-829885-f9b40bc8@whatdotheyknow.com

Date: 23<sup>rd</sup> March 2022

Dear Rob Davies

**FREEDOM OF INFORMATION APPLICATION REFERENCE NO: DPO/FOI/000431/22**

Thank you for your request for information received by Lancashire Constabulary on 03/02/2022 which was as follows:

***I am writing to request information which I believe is held by the Regional Organised Crime Unit or Special Operations Unit (ROCU/SOU) of which your force is part. I believe I am entitled to this information under the Freedom of Information Act 2000.***

***I draw your attention to a previous FOI answered by West Midlands police (Ref: Cryptocurrency 1218A/21), to indicate that such information is held - and was disclosed - by at least one ROCU and might therefore be reasonably expected to be held - and disclosed - by others.***

***I would like to know the following:-***

- 1. How much cryptocurrency has been seized by your force, or the ROCU of which it is part, since 2017. Please provide a breakdown by year and by the type of cryptocurrency (e.g. Bitcoin, Ethereum etc)***
- 2. How much has been returned to the subjects of any seizure (again, by date and type please).***
- 3. How do you store cryptocurrency that you have seized?***
- 4. In cases where seized cryptocurrency is not returned, what happens to it?***

***I look forward to receiving a response within the statutory period.***

Section 1 of the Freedom of Information Act 2000 (FOIA) places two duties on public authorities. Unless exemptions apply, the first duty at s1(1)(a) is to confirm whether the information specified in a request is held. The second duty at s1(1)(b) is to disclose information that has been confirmed as being held. Where exemptions are relied upon Section 17 of the FOIA requires that we provide the applicant with a notice which: a) states that fact; b) specifies the exemptions in question and c) state (if that would not otherwise be apparent) why the exemption(s) applies.

Your request has now been considered and the information you are seeking is held but some of the information cannot be provided at this time:

Unfortunately, the amount of cryptocurrency seized by the Lancashire Constabulary requested in question 1 and the location where the cryptocurrency is stored requested in question 3 is found to be exempt from disclosure under the Freedom of Information Act 2000 by virtue of the listed exemption:

- **Section 31(1)(a)(b) – Law Enforcement**

This is a qualified and prejudice-based exemption, and as such it is necessary for us to consider both the harm which would be caused by the disclosure and the public interest factors both for and against the disclosure. Details of these can be found below.

## **Evidence of Harm**

Policing is an information-led activity, and information assurance (which includes information security) is fundamental to how the Police Service manages the challenges faced. In order to comply with statutory requirements, the College of Policing Authorised Professional Practice for Information Assurance has been put in place to ensure the delivery of core operational policing by providing appropriate and consistent protection for the information assets of member organisations, see below link:

<https://www.app.college.police.uk/app-content/information-management/>

It is widely recognised that criminals use Cryptocurrency to take advantage from the perceived anonymity of digital assets for illicit purposes. Cryptocurrency transactions can also be for vast amounts.

It is accepted that there has been information previously released into the public domain that confirms the amount of Cryptocurrency seized under law enforcement purposes. However, a motivated actor with the right tools can use this information, using methods that map out exactly where the funds may have originated from, confirming that they have been seized and that criminality had been identified. Therefore, there exists a risk of forewarning criminals which in turn could jeopardise investigations if there are outstanding suspects or funds that have yet to be seized or restrained.

Commercial Service Providers are vitally important in the Criminal Justice system and they play a crucial role by supporting UK Policing with expertise and solutions. Cryptocurrency when seized as part of a criminal investigation requires suitable, secure storage, which can include use of a third-party commercial service provider. Whilst not in any way questioning the motives of the applicant, it must be taken into account when considering potential harm that a disclosure under the Freedom of Information Act 2000 is made to the world at large, rather than a private correspondence. Specific details of any outsourced Cryptocurrency storage solution used by the Lancashire Constabulary would be extremely useful to those involved in criminality as it would enable them to create a map of those most used by police forces.

Commercial providers can also be targeted by malicious actors, for example the below unofficial article relates to the kidnapping of an employee of a UK based cryptocurrency exchange:

<https://www.reuters.com/article/uk-ukraine-kidnapping-idUKKBN1EN1QE?msclid=6182f897a69d11ec97e091da8be80833>

The above incident is not the only one of its kind. As such, providing information to the wider public about the volume of assets stored and where they are stored increases the risk of cyber-attacks, insider threat and other hostile actions by those who may wish to infiltrate either the supplier or law enforcement. The size of the assets that have been seized is significant and the Lancashire Constabulary takes the security of these assets extremely seriously.

By providing a list of Commercial Service providers, Force by Force, a malign individual could identify those most critical to the Law-and-Order sector and specifically target those proving the most assistance. This would have a huge impact on the effective delivery of operational law enforcement as it would leave companies open to further cyberattacks which could have devastating consequences for law enforcement.

## **Factors favouring Disclosure**

Confirming the size of seized Cryptocurrency transactions along with the names of Commercial Service Providers in respect of Cryptocurrency Storage solutions would be of interest to the public, namely give insight into the processes used to solve crimes and widen public discussion on such matters.

## **Factors favouring Non-Disclosure**

Measures are put in place to protect the community we serve and as evidenced within the harm, to

provide a size of Cryptocurrency seizures along with a detailed list of Commercial Service Providers would allow individuals intent on disrupting law enforcement from targeting specific organised crime gangs, and criminality overall; using the information obtained to maximise the impact.

Taking into account the security climate within the United Kingdom, and the sensitive nature of criminal investigations, no information which may aid criminality should be disclosed. It is clear that it would have an impact on a Force's ability to carry out the core duty of enforcing the law and serving the community.

The public entrust the Police Service to make appropriate decisions with regard to their safety and protection and the only way of reducing risk is to be cautious with what is placed into the public domain.

### **Balance Test**

The Police Service is charged with enforcing the law, preventing and detecting crime and protecting the communities we serve. In order to effectively and robustly carry out those duties, external services are utilised which are vital to investigating criminal activity. Weakening the mechanisms used to investigate any type of criminal activity would have a detrimental impact on law enforcement as a whole. To provide the overall sums of Cryptocurrency seizures along with the names of any Commercial Service Providers within the context of Cryptocurrency storage solutions, despite the known risks of cyber-attacks would undermine any trust or confidence the public have in the Police Service. Therefore, at this moment in time, it is our opinion that the balance test favours against the disclosure of the information requested.

This letter therefore serves to act as a refusal notice for these aspects of your request, as per S.17 (1) of the Act.

### **Question 1**

- 1. How much cryptocurrency has been seized by your force, or the ROCU of which it is part, since 2017. Please provide a breakdown by year and by the type of cryptocurrency (e.g. Bitcoin, Ethereum etc)***

<b>Year</b>	<b>Type</b>
2019	Bitcoin
2020	Bitcoin
2021	Bitcoin

- 2. How much has been returned to the subjects of any seizure (again, by date and type please).***

The Lancashire Constabulary has not returned any cryptocurrency.

- 3. How do you store cryptocurrency that you have seized?***

Please see the above exemption - Section 31(1)(a)(b) – Law Enforcement.

- 4. In cases where seized cryptocurrency is not returned, what happens to it?***

Section 84 of the Proceeds of Crime Act (2002) gives a definition as to what is classed as property under the act, which includes “things in action and other intangible or incorporeal property.” Cryptocurrencies therefore fall into this definition, giving the powers under the Act to treat Cryptocurrency as property.

Sections 47A through to S47R of the act give powers of search and seizure, in which Cryptocurrency can be seized, including initial detention and further detention powers prior to a restraint order being

obtained. Restrained assets are held until any potential conviction and subsequent confiscation order made, which is done post-conviction. Should a criminal case not be successful, assets may be returned to the owner. In addition, the defendant may wish to raise funds for the confiscation order via other assets at their disposal, in which case the cryptocurrency can also be returned.

If you are unhappy with the service you have received in relation to your request and wish to make a complaint or request an internal review of our decision, you should write to the Data Protection Officer, Data Protection Office, Police Headquarters, Saunders Lane, Hutton, Preston PR4 5SB or alternatively send an email to [FOI@lancashire.police.uk](mailto:FOI@lancashire.police.uk). Details of the Constabulary's Freedom of Information Complaint Procedures can be found attached to this email.

If you are not content with the outcome of your complaint, you may apply directly to the Information Commissioner for a decision. Generally, the Information Commissioner's Office cannot make a decision unless you have exhausted the complaints procedure provided by Lancashire Constabulary. The Information Commissioner can be contacted via the following link:

<https://ico.org.uk/global/contact-us/> or by telephone on 0303 123 1113.

The Information Commissioner's Office request that you do not contact them by post during the Coronavirus pandemic as their offices are closed.

Yours sincerely

**Information Access Team**

Data Protection Office