Dear R Davies,

REQUEST

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 Midland 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?

RESPONSE

In regards to question 1 – 3 I can confirm that this information to answer these questions is held but is exempt by virtue of section 31.

The Harm Test process requires Cheshire Constabulary to consider any possible harm that might arise as a result of placing the requested information into the public domain. This process considers the potential harm to:

- Individuals
- The community as a whole
- Cheshire Constabulary and the wider policing service
- Other bodies

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 Cheshire 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:

Ukraine kidnappers free bitcoin analyst after $1 million ransom paid | Reuters

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 Cheshire 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.

However in response to question 1 we can confirm the types of cryptocurrency seized include Bitcoin and Monero.

Regards,

Lucy Taylor – Request Decision Maker
Cheshire Constabulary and Cheshire Fire & Rescue Service Joint Corporate Services
Clemonds Hey | Oakmere Road | Winsford | Cheshire | CW7 2UA
Visit www.cheshire.police.uk | www.cheshirefire.gov.uk
Follow @cheshirepolice and @CheshireFire on Twitter
Like Cheshire Police and Cheshire Fire and Rescue Service on Facebook