Burn-and-remint: a new tool in cryptoasset recovery?



© Getty Images/iStockphoto

Could a bold interpretation of the new powers contained in Part 5 of the Proceeds of Crime Act 2002 provide a silver bullet for law enforcement? Ashley Fairbrother, Joe Nahal-Macdonald & Sarah Wood set out the case

IN BRIEF

▶ This article considers the new powers contained within Pt 5 of the Proceeds of Crime Act 2002, and whether UK law enforcement should harness the cryptocurrency Tether's 'burn-and-remint' mechanism to help victims to recover stolen assets.

▶ The authors consider that the criteria to be satisfied in order for these new powers to be used are met, and moreover that there is likely to be a willingness by both law enforcement and the courts to adopt a purposive interpretation to these powers.

With effect from 26 April 2024, the Economic Crime and Corporate Transparency Act 2023 introduced new powers into Pt 5 of the Proceeds of Crime Act 2002 (POCA 2002) providing for the seizure, detention, freezing and forfeiture of cryptoassets and related items. These powers are exercisable by the magistrates' court.

This article considers those powers and whether UK law enforcement should harness the cryptocurrency Tether's 'burn-and-remint' mechanism to help victims to recover stolen assets, in the manner that the authors have successfully experienced with US law enforcement. We address whether Tether, as a stablecoin issuer, could be classified as a 'cryptoasset service provider' under s 303Z35(1)(c), POCA 2002, to provide a silver bullet for law enforcement asset recovery.

The article highlights that legislators cannot foresee all the possible combinations of circumstances the future may bring, and they were undoubtedly unaware of the possibility of 'burn-and-reminting' digital assets when drafting the new Pt 5, POCA 2002 powers less than a year ago, such is the rapid pace of learning in this space. It is the difficulty in anticipating for legislators that brings relative indeterminacy of aim in legislation, and now a choice has to be made by UK law enforcement to determine the legislation's meaning and purpose; we do not live in a world suitable for mechanical jurisprudence when it comes to financial crime, and the authors suggest that the choice by law enforcement must be purposive constructive of legislation, to use their most powerful weapon—POCA 2002—to tackle fraudsters and help their victims, which US law enforcement has shown no hesitation in doing.

Background on burn-and-remint

Tether is the largest cryptocurrency in terms of trading volume, and pegged against the US dollar, accounts for a circa 70% market share among so-called 'stablecoins'. Tether Limited, a company based in the British Virgin Islands, facilitates the issuance, redemption, and management of its USDT digital asset, including through its burn-and-remint system. Tether has the ability to destroy tokens (burning) and issue new ones (minting) to manage supply or adjust token balances across different blockchains to help maintain the token's peg to the US dollar and ensure liquidity across different blockchain networks.

While Tether's burn-and-remint mechanism is integral to its operations, a helpful consequence of this function is that it can allow Tether to freeze and reissue tokens in cases of fraud or theft, offering an asset recovery tool that could be crucial for law enforcement operations.

Freezing & seizure powers

Under the amended powers within POCA 2002, an 'enforcement officer' can freeze and apply to seize assets associated with criminal activity, primarily targeting custodial wallets or exchanges with UK connections. Section 303Z36, POCA 2002 provides the basis for crypto wallet freezing orders, and sub-s (1) outlines the grounds for exercise of the power:

> '(1) This section applies if an enforcement officer has reasonable grounds for suspecting that cryptoassets held in a crypto wallet administered by a *UK-connected cryptoasset service provider* [emphasis added]
> (a) are recoverable property, *or*
> (b) are intended by any person for use in unlawful conduct.'

It is useful to consider whether assets in custodial or non-custodial wallets might be recoverable under the new power. Broadly, in the former category the owner is not in possession of the cryptoasset private keys—they are hosted by a third-party exchange such as Coinbase. In the latter category, the owner maintains their private key. While custodial wallet providers have long been an amenable partner to law enforcement applications, successful recovery via a non-custodial wallet is usually more difficult, not least due to the need for corroboratory 'offline' data (ie physical evidence under searches, such as a private key written down). The writers submit that the new power will offer a potential avenue, notwithstanding Tether does not fall under the traditional example of 'an exchange'.

There are two criteria that must be satisfied for law enforcement to use the new powers for asset recovery and to help victims:
(1) Is Tether a 'cryptoasset service provider'?
(2) Is Tether 'acting in the course of business

in the UK'?

We examine those questions below, and consider both tests are met.

Is Tether a 'cryptoasset service provider'?

Section 303Z35, POCA 2002 provides the definitions which underpin the operative wording in s 303Z36—ie what is a 'cryptoasset service provider'.

Pursuant to sub-s (1)(c), a 'cryptoasset service provider includes *cryptoasset exchange provider* and custodian wallet provider'.

Pursuant to sub-s (1)(a):

> 'a "cryptoasset exchange provider" means a firm or sole practitioner who by way of business provides one or more of the following services, *including* where the firm or sole practitioner does so as *creator or issuer of any of the cryptoassets* involved—
> (i) …
> (ii) exchanging, or arranging or making arrangements with a view to the *exchange* of, *one cryptoasset for another*, …'

In applying these criteria:

a. Tether is plainly a 'creator' and/or 'issuer' of the cryptoasset USDT and therefore meets the definition of a 'cryptoasset service provider' under s 303Z35, POCA 2002 as it actively facilitates the issuance, redemption, and management of its stablecoin, even if it is not a direct custodian or exchange provider.
b. Tether's 'burn-and-remint' facility, which is integral to Tether's operations, constitutes exchanging one cryptoasset for another—indeed that is its very purpose (ie coin A is burned and reminted, it *becomes* coin B, and this is an *exchange* of assets) per sub-s (1)(a)(ii) above.

With these criteria clearly met, it must then be established that Tether is acting in the course of a business in the UK.

'Acting in the course of business in the UK'

Pursuant to s 303Z36(8), POCA 2002, a cryptoasset service provider must be a 'UK-connected cryptoasset service provider', and the definition of a 'UK-connected cryptoasset service provider' is unsurprisingly broad. Pursuant to sub-s (a), simply 'acting in the course of business carried on by it in the United Kingdom' is sufficient.

It is notable that UK users can go to the Tether homepage, sign up for a Tether account within seconds, and begin to trade USDT. Given that UK citizens can invest in, convert and exchange USDT, and benefit from Tether's smart contract on multiple blockchains, such widespread access plainly shows that Tether's activities fit the jurisdictional hook.

Crucially, Tether's terms of service do not prohibit the use of its services by UK citizens, as it does with other nationalities, such as 'US Persons'. Para 3.1–3.5 of Tether's terms of service prohibit the use of its services by 'US Persons', which are defined at para 1.1.4.7 to include US citizens or US residents. Moreover, Tether's record of proactive cooperation with law enforcement worldwide indicates that it is unlikely to contest such applications in appropriate cases. Tether is showing itself to be a leading light in the crypto industry for being on the right side of justice and support for its users and victims. The optics of it attempting to avoid assisting victims by taking a technical or mechanical interpretation point that it is *not* acting in the course of a business in the UK would be a *volte face* from its recent approach.

Ultimately however, this is a matter of judicial discretion. Law enforcement officers' applications will aim to persuade the courts that where the victim is based in the UK and their recoverable property stored in USDT and readily identifiable, the circumstances would lend support for the court to make an order facilitating recovery.

Support for a purposive interpretation

In support of the courts adopting the same interpretation as above, are the existing jurisprudence and legal frameworks lending a purposive interpretation to both addressing financial crime and helping the victims of cryptoasset-based fraud?

Case law on statutory interpretation

Law enforcement will be familiar with the well-known case of *R v Waya* [2012] UKSC 51, in which the Supreme Court mandated a purposive approach to statutory interpretation when addressing financial crime, stating 'statutory language must be given a fair and purposive construction in order to give effect to its legislative policy'. The legislative intent in introducing the new Pt 5, POCA 2002 powers was to combat fraud and illicit activity, and in the authors' view a purposive interpretation of the legislation must be construed to include Tether.

Relevant regulatory guidance

The EU's Markets in Crypto-Assets (MiCA) regulations recognise stablecoin issuers as key players in cryptoasset markets, suggesting that their role should be viewed broadly. This regulatory context aligns with a purposive interpretation in a modern crypto-based world, which is subject to rapid change.

Policy considerations

The broader objective of POCA 2002 is to prevent the use of criminal assets, and to identify, seize and mulct those assets from criminal networks and defendants, whether known or unknown. Aligning POCA 2002's powers to Tether's burn-and-remint capabilities would further this aim by providing a pathway for asset recovery, particularly in cases involving fraud or theft in the crypto space.

Practical considerations

In summary, there is likely to be a willingness by both law enforcement and the courts to adopt a purposive interpretation to the Pt 5, POCA 2002 powers; furthermore, Tether's proactive stance in collaborating with law enforcement globally, often working alongside authorities to investigate crypto-related crimes, suggests that it would support a purposive interpretation enabling asset recovery.

In the authors' view, this is likely to work even more seamlessly if a state-level agreement is reached between UK authorities and Tether, as we understand has been agreed with US state authorities. There are benefits to both sides—providers seek legitimacy and uptake, while states want to combat financial crime; such aims are not mutually exclusive.

In cases where the suspect appropriating USDT cannot be identified, there may be minimal practical opposition to the innovative use of the new powers by law enforcement. As a further precaution, victims and law enforcement could attempt to serve proceedings on USDT address holders via non-fungible tokens, which, while unlikely to elicit a response in most cases, could bolster confidence among law enforcement, Tether, and the courts to implement a burn-and-remint process to assist victims.

This tool could significantly enhance UK law enforcement authorities' ability to combat crypto-related crime and recover assets for victims, thereby strengthening the UK's regulatory framework, aligning with US law enforcement practices, and providing robust enforcement of Parliament's intention to support victim asset recovery. NLJ

Ashley Fairbrother, partner, & **Joe Nahal-Macdonald,** senior associate at Edmonds Marshall McMahon (*emmlegal.com*), & **Sarah Wood,** barrister at 5 St Andrews Hill (*5sah.co.uk*). *Newlawjournal.co.uk*