DEVELOPMENTS IN THE FIGHT AGAINST CRYPTO-FRAUD IN 2020

Authored by: Jennifer Craven & Jasmin Khalifa, Pinsent Masons

It is more than 10 years ago since the first bitcoin was mined. Since then, we have seen the rise of other cryptocurrencies in the form of Ethereum, Litecoin and Ripple, and the use of cryptoassets as a means of currency has developed exponentially. Yet, the use of cryptoassets continues to be synonymous with shady schemes and bad investments, and 2020 sees no let up: crypto scams are said to be skyrocketing. According to one report[1], 2020 is set to be one of the highest in cryptoasset fraud, with the first five months of 2020 recording that crypto-fraud already totalled USD $1.36 billion.

The likely impact of COVID-19 on these statistics cannot be underestimated. According to the US Federal Bureau of Investigations, cyber-criminals have leveraged increased fear and uncertainty during the pandemic to steal money and launder it through complex cryptocurrency ecosystems. They warned that fraudsters are on the verge of unleashing a massive wave of cryptoasset scams relating to coronavirus. Similar warnings were given by the UK's Financial Conduct Authority (FCA) and the City of London Police's National Fraud Intelligence Bureau. Several kinds of scams, orchestrated via cryptoassets are anticipated to become increasingly popular in the wake of the coronavirus, including "work from home scams," "blackmail attempts," and "investment scams". Many are executed by tricking victims off legitimate platforms into illicit chat rooms where cryptoasset payment is requested, paid and, in many cases, never seen again.

All of this will be disappointing news to financial crime enforcement agencies and market regulators. January 2020, saw new regulatory powers introduced to allow the FCA to supervise how cryptoasset businesses manage the risk of money laundering and counter-terrorist financing. However, there are gaps in their powers: they do not cover how cryptoasset businesses conduct their business with consumers and the FCA is not responsible for ensuring that cryptoasset businesses protect client assets. Recently, the response of Action Fraud, which partners the FCA and is overseen by the City of London police, has been strongly criticised: the national reporting service was thrust into the limelight last year when an undercover Times investigation revealed that victims were mocked by call handlers as "morons", and that call handlers were trained to mislead victims into thinking their cases would be investigated when most were never looked at again.

An arguably more effective area of development in the fight against crypto-fraud is that currently being routed in the UK Courts. In November 2019, the UK Jurisdiction Taskforce

[1] *2012 EWHC 1056 (Ch)*

(UKJT) published the Legal Statement on Cryptocurrency and Smart Contracts. The Legal Statement, which was that cryptoassets fell into the legal definition of "property", was fundamental in providing much wanted legal certainty: people who are defrauded of their cryptoassets, have them stolen by hackers, or are the victim of more 'traditional' frauds, the proceeds of which are then laundered through cryptocurrency exchanges, are less likely to be able to recover their losses if cryptoassets are not considered to be 'property'.

The Legal Statement provided authoritative, albeit not binding analysis but, subsequent UK cases have endorsed the definition of cryptoassets as "property". Earlier this year, in AA v Persons Unknown [2019] EWHC 3556 (Comm), Mr Justice Bryan specifically held, on a without notice application, that cryptoassets were "property" for the purposes of granting proprietary or freezing injunctive relief. In this case, the court in London issued an injunction requiring a bitcoin exchange to help an insurance company recover funds it paid to hackers. The proprietary injunction, among other things, required the exchange to disclose information that could help the insurer identify those responsible for carrying out a ransomware attack on one of its customers, and to prevent bitcoin traced from the ransom payment being moved from the exchange's account. The case demonstrates that businesses and individuals who have become a victim of fraud and malware attacks, and have paid ransom monies – whether in fiat currency or cryptocurrency – can seek to trace the payment of those monies even where the fraudsters are unknown, using various civil fraud and High Court remedies available.

More recently, on 29 July 2020, in Toma & True v Murray [2020] EWHC 2295 (Ch), in a case involving a bitcoin transaction that went wrong owing to a fraud, and which left the Claimants sans bitcoin, Mr Robin Vos, (although endorsing the test for a proprietary injunction as set out in AA v Unknown Persons) refused to continue the proprietary injunction. The Claimants, by their own admission, would have had difficulty satisfying any cross-undertaking to damages and the claim was one which was capable of being satisfied in monetary terms rather than relying on a proprietary remedy. In this regard, it was noted that (in contrast to the position in AA v Persons Unknown) the Defendant was identified, and had shown he held a significant unencumbered asset, so there was no reason to suppose that he would not be able to meet any award made against him.

In contrast, in the case of Blockchain Optimization S.A. and others v LFE Market Ltd and others [2020] EWHC 2027 (Comm), the Commercial Court continued a freezing injunction against Defendants who had allegedly fraudulently misrepresented investors to invest in a cryptocurrency platform, signalling the UK Court's tough approach to suspected investment fraud.

Both cases are further evidence of the upwards trend in crypto related litigation being fought in the UK Courts. A similar trend is seen in other common law jurisdictions. The Singapore International Commercial Court in B2C2 Ltd v Quoine PTC Ltd [2019] SGHC (I) 03, and which was followed on appeal [2020] SGCA(I) 02 at [144], held that that cryptocurrencies fulfilled Lord Wilberforce's classic definition, so as to amount to "property" in a generic sense. More recently, in Ruscoe v Cryptopia Ltd (in liq) [2020] NZHC 728, the High Court of New Zealand held that digital assets of a cryptocurrency exchange constituted "property" and were held on trusts for accountholders on that exchange.

Undoubtedly, the use of cryptocurrency is likely to remain a playground for fraud for the remainder of 2020 and beyond. That said, victims can take some comfort from recent developments in common law jurisdictions. In particular, the UK Court has so far shown itself to be an adaptable and effective forum in the fight against crypto-fraud. It is willing to use the application of traditional civil remedies which might assist in the tracing exercise such as injunctive relief in the form of freezing orders, even in circumstances where the victim cannot identify the fraudster, so as to prevent further dealing with the cryptoasset. A tough approach is to be welcomed.