KEY POINTS

- Victims of crypto fraud are assisted by recent case law confirming the availability of interim relief against third parties and a range of possible causes of action against fraudsters.
- If a victim's cryptoassets are traceable to an exchange and have been frozen, enforcement of a judgment against the fraudsters should be possible against the cryptoassets frozen by the exchange.
- Victims should consider their legal position carefully before making proprietary claims directly against exchanges, especially if the exchange uses pooled accounts or "hot wallets".

Feature

Author Gretel Scott

Remedies for victims of crypto fraud

In this article, Gretel Scott discusses the possible remedies and methods of enforcement for victims of crypto fraud.

THE PROBLEM

Your client (C) contacts you urgently: they have fallen victim to a cryptoasset fraud and lost their savings. The identity of the fraudsters is unknown other than an email address and public wallet details.

You recount the law on cryptocurrencies being treated as property, disclosure orders against exchanges, engaging an expert in blockchain analytics to trace the crypto, and freezing and proprietary injunctions against the unknown fraudsters and exchanges. But what the client really wants to know is what do they receive at the end of it. Without successful enforcement, it is a pyrrhic victory. As Lord Bingham said in *Société Eram Shipping Co Ltd v Cie Internationale de Navigation* [2004] 1 AC 260 at 267:

> "… it is one thing to recover a favourable judgment; it may prove quite another to enforce it against an unscrupulous defendant."

This article follows the typical journey of a crypto fraud claim and traverses interim remedies and personal and proprietary claims before concluding with enforcement.

INTERIM RELIEF AND SERVICE

The first step in a cryptoasset claim is usually for C to trace the transfer of their cryptoassets, often using an investigator to study the public distributed ledger. C can then apply for disclosure of information orders against those persons, such as exchanges, identified in the tracing exercise.

Various applications for interim remedies have been brought by crypto fraud victims in the English courts in the past few years. In summary, these judgments have held that:

- Cryptocurrencies are property: *AA v Persons Unknown* [2020] 4 WLR 35, *Fetch.AI v Persons Unknown* [2021] EWHC 2254 (Comm)). It is at least realistically arguable that a non-fungible token (NFT) should be treated as property as well: *Osbourne v Persons Unknown* [2023] EWHC 39 (KB). The Law Commission recommends that cryptocurrencies and NFTs are recognised as "third category things" (Digital Assets, Final Report, 28 June 2023).
- The *situs* (location) of the cryptoasset may be England if that is the country where the owners are domiciled or resident (this being the place where the cryptoasset is controlled, usually by knowledge of the private key): *Fetch.AI* and *Tulip Trading v Bitcoin Association for BSV* [2022] EWHC 667 and [2023] EWCA Civ 83. This raises various jurisdictional issues worthy of a separate article.
- Victims can obtain a worldwide freezing order (with ancillary information orders) and a proprietary injunction against persons associated with the victim's cryptocurrency or its traceable proceeds: *Fetch.AI*.
- With the new gateway under CPR PD6B para 3.1(25), now both *Norwich Pharmacal* and *Bankers Trust* orders can be served outside the jurisdiction: *LMN v Bitflyer Holdings Inc* [2022] EWHC 2954 (Comm). Other gateways commonly used by victims are gateway:
  - 3 (anchor defendant);
  - 4A (further claim out of the same or closely connected facts);
  - 9 (damage within the jurisdiction);
  - 11 (property in the jurisdiction);
  - 15 (constructive trustee arising out of acts or assets in the jurisdiction); and
  - 16 (restitution for enrichment within the jurisdiction).
- The courts will grant service out of the jurisdiction where the location of the defendants is unknown, and service can be by alternative means under CPR r 6.15: *D'Aloia v Persons Unknown* [2022] EWHC 1723 (Ch) (service via NFT on the blockchain and by email).
- Applications for interim relief may be made without notice to the defendants, but since Trower J's judgment in *Piroozzadeh v Persons Unknown* [2023] EWHC 1024 (Ch), victims should be cautious of applying without notice against exchanges where no wrongdoing is alleged. C should consider serving any order on the exchange as a non-respondent instead.
- Some tokens, such as Tether, can be frozen by their operating companies which is beneficial for victims as it means these cryptocurrencies do not need to reach an exchange in order to be frozen, although the operating company will likely require a court order: *Reyes v Persons Unknown* [2021] EWHC 1938 (Comm).

CAUSES OF ACTION

Proprietary claims

Generally, the most useful remedy for victims of crypto fraud is to bring a proprietary claim against the fraudsters and, depending on the circumstances, against the exchange. As a proprietary claim rather than a personal claim, the victim benefits from familiar advantages including priority in insolvency, the ability to recover the property itself or an equitable lien for the amount the property was worth when it was taken (which may be beneficial in a volatile market) and recovery from subsequent transferees.

A proprietary claim relies on C having some proprietary interest in the cryptoassets in the defendant's hands. There are two different types

of fraud which may have been perpetrated on C. The first is where C is fraudulently induced to transfer their cryptoassets, believing it is for a valid investment opportunity (category 1). The second is where C's cryptoassets are stolen and transferred without C's consent, for example by hacking C's computer and obtaining the private key (category 2).

In category 1 fraud, legal title passes as C consents to the transfer, but C has a mere equity to rescind which will become an equitable proprietary right if C chooses to enforce it. This means that a subsequent recipient will be deemed a constructive trustee of the cryptoasset. Whether the exchange (rather than its customer) has legal title to the cryptoassets is doctrinally controversial but the exchange at least has the power to return control of the cryptoassets to C. In category 2 fraud, C may rely on a proprietary claim to vindicate its subsisting legal title in the stolen cryptoassets and/or a constructive trust may arise as soon as the cryptoasset is received by the fraudster as in *Westdeutsche Landesbank Girozentrale v Islington London Borough Council* [1996] AC 669, though again this is not without doctrinal criticism.

Personal claims

As against the fraudsters, there is a range of potentially relevant personal claims including misrepresentation, deceit, restitution for unjust enrichment, breach of confidence, conspiracy and conversion (of the hardware or document that recorded C's private key; not of any intangible).

If C can establish a breach of trust (such as arising from the above-mentioned constructive trust) or breach of fiduciary duty, then C may wish to claim against a third party for dishonest assistance or knowing/unconscionable receipt. Relevant considerations would include:

- (for dishonest assistance) whether D was dishonest, which is an objective test but assessed in light of what a person actually knew at the time (suspicion based on specific facts, rather than speculative suspicion, combined with a deliberate decision not to ask questions, will suffice);
- (for knowing receipt) whether D received the cryptoassets for its own account (ie beneficially), which may not be the case with some crypto platforms if they act as agent; and
- (for knowing receipt) whether D acted unconscionably, which generally means showing that the recipient knew enough about the facts to make it unconscionable for it to retain the assets (which is a lower test than for dishonest assistance).
- (for knowing receipt) whether C has to prove a continuing proprietary interest in the crypto transferred to D to render D's receipt unconscionable (which may be difficult where foreign law intervenes) – the Supreme Court's future decision in the appeal of *Byers v Saudi National Bank* [2022] EWCA Civ 43 will be relevant to this.

An exchange may be assisted by the commercial context and the fact that the blockchain does not record the circumstances of each transaction.

Where C held its cryptoassets with a particular exchange or custodian, C may consider whether the facts permit bringing the following claims directly against the exchange or custodian:

- Breach of contract, but the contract is often governed by foreign law with an arbitration clause.
- Breach of trust or fiduciary duty. In *Wang v Darby* [2021] EWHC 3125 (Comm), the court indicated that digital assets could be held on trust (and see *Ruscoe & Moore v Cryptopia Ltd (in liquidation)* [2020] NZHC 728 (NZ) which decided that the Cryptopia exchange held the digital assets of its customers under an express trust).
- There has been much speculation about whether a claim may also be possible relying on *Barclays Bank v Quincecare* [1992] 4 All ER 363. C would need to show that the exchange/custodial service provider had clear knowledge (or was put on inquiry) that the proposed transaction was in reality an attempt to defraud the customer and so should have refused to exercise the order. Although Falk J was unpersuaded by this claim in *Tulip Trading*, permission to serve out has now been granted by the Court of Appeal and the point may be tested at trial in due course. Following the Supreme Court's decision in *Philipp v Barclays Bank* [2023] UKSC 25, *Quincecare* will be even harder to apply in crypto cases. The Supreme Court held that it does not apply in "authorised push payment" fraud but is instead confined to cases where the bank has reasonable grounds to believe that a payment instruction given by an agent is an attempt to defraud the customer (or in limited other situations where there is an absence of authority).

Victims may try to be more creative and look beyond the fraudsters and the recipient exchanges. Potential wider defendants include the wallet provider for breach of contract for a software defect which exposed C's crypto to a hack, or the software developers of the bitcoin network for dishonest assistance or breach of a duty of care. C could also investigate an exchange's insurance (eg Binance has a "Secure Asset Fund for Users" which it describes as an "emergency insurance fund").

OVERCOMING PROBLEMS WITH TRACING AND THE BONA FIDE PURCHASER DEFENCE

Cryptoassets can often be traced from one holder to another, assisted by the public ledgers. However, sometimes this can be complicated by techniques such as chain-hopping (swapping cryptocurrencies from one token to another), pooling wallets and empty wallets.

These features will not necessarily defeat C's claim. For example, whilst tokens based on fungible standards will be hard to trace if mixed, some cryptocoins record a unique transactional history and for those that do not, the terms of the mixer service contract may allow one token to be attributed to another, or conventional rules for tracing into mixed funds could be applied (including "first in first out", "rolling charge", or withdrawals borne rateably by all contributors). Crypto held in pooled accounts may nevertheless be held on trust for a group of users (with users being co-owners of the fund). As for empty wallets, a fraudster may hold several different wallets with an exchange, allowing C to trace

into a different wallet with a positive balance. The UK's implementation of the FATF travel rule on 1 September 2023 (reg 5 of the Money Laundering and Terrorist Financing (Amendment) (No.2) Regulations 2022) should also assist victims as it will require exchanges to share certain transactional and personal information relating to the sender and the buyer in cryptoasset transfers over €1,000.

As for the bona fide purchaser (BFP) defence, this is relevant in category 1 fraud where the transferee of C's cryptoassets acquires legal title to the property but subject to C's equitable claim unless the transferee satisfies the BFP defence. There are three requirements for the equitable bona fide purchaser defence:

(1) receipt without notice of a breach of trust;
(2) valuable consideration for the receipt of funds (which means more than just opening an account or giving credit – see *Lipkin Gorman v Karpnale Ltd* [1991] 2 AC 548) such that the recipient is deemed to be a "purchaser"; and
(3) good faith.

In *Piroozzadeh*, Binance relied on evidence that the user did not retain any property in the cryptocurrency deposited. Instead, the user's account was credited with the amount of the deposit and they were permitted to draw against the credit balance (operating like a traditional bank in crediting and debiting accounts, although because cryptocurrencies are not recognised legally as money, the Law Commission recommends that the exchange's obligation to pay is better characterised as a claim for unliquidated damages for failure to deliver, rather than a monetary debt). The cryptoassets were then swept into a central unsegregated pool address (a "hot wallet") where they were treated as the exchange's assets and transactions are made in and out of the central pool. Trower J said that "if the recipient of the stolen Tether was a bona fide purchaser, it is almost certainly the case that the proprietary rights of the beneficiary will not survive". As the Law Commission observes, the equitable defence requires executed consideration if the defendant is to be a "purchaser" but on the facts, the Binance accounts had been emptied (ie the credit had been used rather than just granted).

Following *Piroozzadeh*, the equitable BFP defence is certainly a problem for victims of crypto fraud if their cryptoassets have passed through an exchange which pools crypto and/or uses hot wallets. However, there are various mitigating factors.

First, unless a special defence of good faith purchaser for value without notice were developed for crypto tokens as the Law Commission has recommended, the BFP defence is only relevant to consensual transfers (category 2 fraud). If the cryptoassets were stolen or otherwise misappropriated (category 1 fraud), legal title does not pass so there can be no BFP defence and the maxim *nemo dat quod non habet* applies.

Second, the burden of proving the defence is on the defendant.

Third, if C's crypto is traceable to segregated ("self-custodial") wallets then the exchange may not satisfy the "purchaser" requirement as the exchange is unlikely to be the legal owner of the cryptoassets.

Fourth, in some circumstances exchanges may have notice, for example if they are involved in the fraud, or if the fraud has already been reported by another victim before C is targeted. C may also be able to show that coins known to be stolen are clustered with certain public keys such that all coins associated with the same public key might be tainted (although simply transacting in a chain involving privacy coins or mixers is likely not enough for notice). Under the equitable defence, actual or constructive notice suffices, meaning that the exchange must make inquiries if the facts known to the exchange would give a reasonable exchange in the position of the particular exchange serious cause to question the propriety of the transaction (or put another way, the exchange must seek an explanation if there are features of the transaction such that if left unexplained they are indicative of wrongdoing): *Crédit Agricole Corporation and Investment Bank v Papadimitriou* [2015] 1 W.L.R. 4265. The Law Commission recommends that only actual notice should suffice for the special BFP defence it proposes is developed for crypto.

Fifth, if the private encryption key is stolen by person X located in a different state then there is an argument that like movable property, the laws of that different state will decide whether person X has good title, applying *Winkworth v Christie, Manson and Woods Ltd* [1980] Ch. 496. Therefore, C may be able to plead that a foreign law which does not have an equivalent BFP defence should determine whether C's rights trump a subsequent purchaser's, though note that this argument seems to be untested for crypto and is dependent on which artificial rule is used to determine *situs* for cryptoassets.

Finally, although unlikely to console a victim of fraud in the moment, they could be reminded that the BFP defence may in due course protect them from third parties' claims to other cryptoassets they hold.

ENFORCEMENT

Once the victim's cryptoassets have been located and frozen and judgment obtained against the fraudsters, C will need to decide how best to enforce its judgment. Relevant factors include who holds the cryptoassets (or their traceable proceeds), whether the fraudsters are identified and within the jurisdiction (in which case conventional enforcement methods may suffice), whether the private key is obtainable such that the cryptoassets can be transferred, whether any soft pressure (eg the risk of reputational damage) can be applied to encourage an exchange to comply, and which defendant has the deepest pockets (including if any is insolvent).

To date, the English High Court has granted C the following:

- An order for delivery up of the cryptoassets which are the subject of a proprietary claim, either as against the exchange (*Jones v Persons Unknown* [2022] EWHC 2543 (Comm)) or against the fraudsters but the exchange agrees to co-operate (*Joseph Keen Shing Law v Persons Unknown and Huobi Global Limited* (26 January 2023, unreported)).
- A third-party debt order allowing the victim to take what is owed from whoever has the money. A third-party debt order only applies to "money" or "debt" and

Feature

Biog box
Gretel Scott is a commercial barrister at 3 Verulam Buildings, Gray's Inn, London with a particular interest in actions and remedies arising from civil fraud.
Email: gscott@3vb.com

crypto-tokens are unlikely to be either. However, if a judgment is obtained for a sum in sterling, it seems that it may not matter that the context is crypto – see *Ion Science v Persons Unknown* (28 January 2021, unreported) where a third-party debt order was made by Master Cook against the exchange which owed money to the account holder. Another limitation is that the debt cannot be a foreign debt unless the third-party debt order would be recognised as discharging the third party's liability to the judgment debtor under the foreign law.

- If cryptoassets can be identified in particular wallet holders' accounts (even if mixed and in circumstances where a proprietary claim is difficult) and those accounts are frozen and judgment obtained against those wallet-holders, an order that the cryptoassets subject to the freezing order be transferred into the jurisdiction, converted into Pound Sterling and paid into the Court Funds Office, from which the claimant could apply for an order that the judgment debt be satisfied from the funds under CPR r 72.10 – *Joseph Keen Shing Law*. C may need to provide a cross-undertaking in damages.
- A mandatory injunction requiring code to be written to transfer the cryptocurrency back to the original owner – *Tai Mo Shan Limited v Oazo Apps Limited* (6 March 2023, unreported, EWHC HHJ Pelling KC). It is understood that this was in the specific context of a token bridge where, due to a vulnerability in the code, it was exceptionally possible to reverse the hack by amending the software (in effect, to hack back).

Other options include:

- In *Tulip Trading*, although not tested at the enforcement stage yet, the claimant seeks an order requiring the defendant software developers to implement a software patch enabling it to regain control of the assets, either by transferring the assets to a new address (with a new private key) or by allowing the claimant to regain control of the assets in their existing locations and allocating replacement private keys. The Bitcoin Association for BSV (the first defendant) settled Tulip Trading's claim in June 2022 by agreeing to develop such software. The result (which was already in the process of being developed at the time) is "Blacklist Manager", software for miners which freezes cryptoassets directly on the BSV blockchain (rather than at wallet level) following a court order. The court freezing order is converted to a digital, machine-readable format by recognised notaries. The miners run the Blacklist software (which is an add-on to their node software) which receives the signed freezing order from the notary. When enough miners confirm, it becomes a consensus freeze order and all honest nodes reject any attempt to spend the frozen assets. The Blacklist Manager can also order a re-assignment of the cryptoassets and execute the necessary transactions to transfer the coins to the legally determined owner. Equally, it can recognise and enforce confiscation orders by issuing confiscation transactions at the appropriate block numbers such that once mined, the confiscation transactions cause the frozen currency to be recovered to a recovery agency address. In effect, this works by market pressure as miners who do not run Blacklist Manager or refuse to recognise the freezing order risk having their blocks rejected by the rest of the network.
- If the identity of the fraudsters or the exchange is known but they are not paying, C could obtain information about what assets they hold under CPR Pt 71.
- C could apply to appoint a receiver by way of equitable execution. The receiver is put in the place of the judgment debtor to receive the money. However, this may be expensive.
- An order requiring the defendant marketplace operator to send an NFT to a "burn address", thereby making it redundant, as the Hangzhou Internet Court ordered in the Bigverse case.

CONCLUSION

The cases show that a victim of crypto fraud does have a range of interim and final remedies available, particularly where the victim's assets are successfully traced to an exchange, and the courts will be amenable to developing existing principles to accommodate cryptoasset fraud. Although it can be expensive to bring a claim, it is hoped that the increasing number of cases and the Law Commission's report will bring more certainty and predictability for claimants and defendants alike.

As different cryptoassets vie for popularity, more on-chain tracing and enforcement methods (such as orders to write code or software) may develop. However, this will depend on how the crypto market views legal enforcement. As Birss LJ commented in *Tulip Trading*, remedies requiring code to be amended will test whether the decentralised governance of many cryptoassets is a myth. Some participants may see on-chain enforcement (which effects transfers without the private key) as a threat to the decentralised model and the immutability of the blockchain.

Finally, the cases show that victims are most successful in enforcing where their assets can be traced to an exchange (these also being the cases that victims seem most prepared to litigate). Exchanges may be willing to comply with court orders against fraudsters, but Binance's successful application to discharge the interim proprietary injunction made against it in *Piroozzadeh* shows that victims should be careful how they frame any proprietary claims against exchanges. ■

Further reading:

- The endgame: issues in enforcement against cryptoassets (2022) 8 JIBFL 545.
- Crypto fraud and the bona fide purchaser for value defence (2023) 1 JIBFL 5.
- Lexis+® UK: Banking & Finance: Practice Note: Cryptoassets for dispute resolution lawyers – key and illustrative decisions.