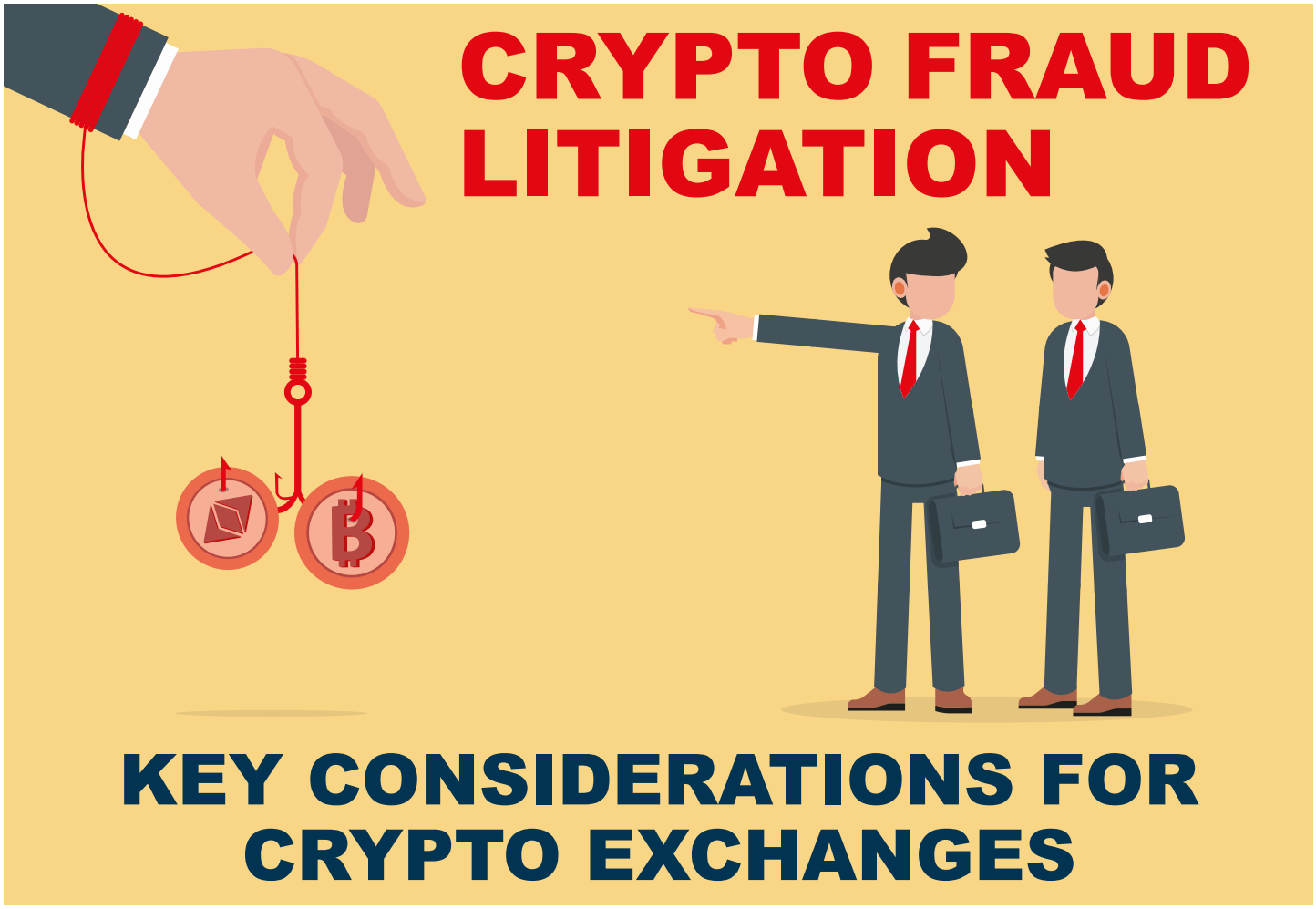

CRYPTO FRAUD LITIGATION

KEY CONSIDERATIONS FOR CRYPTO EXCHANGES

Authored by: Jennifer Craven - Pinsent Masons

There is a lot of legal noise around crypto fraud and what legal remedies exist to help the victim recover crypto that has been stolen, hacked or badly invested. A flurry of English High Court cases show Judges willing to be sympathetic to the plight of victims and demonstrating flexibility, such that the English Courts are often the forum of choice for victims of fraud.

Assuming a victim successfully navigates potential bumps in the road (such as a fraudster's attempts to conceal the crypto by executing complicated transactions known as "peeling" or going "cross-chain"), it is relatively easy to track and trace crypto – much more so than your average fraud involving fiat currency - because the transactional information is there for all to see on the publicly accessible blockchain. This means that in many circumstances the stolen crypto can be traced into an identifiable wallet held at a crypto exchange, often located overseas.

The English legal system, which continues to adapt to meet the needs of victims of crypto fraud, is also changing its rules on the service out of the jurisdiction of a claim for disclosure of information, by introducing a new procedural "gateway" (CPR PD 6B). This will make the process easier for victims to serve disclosure orders on crypto exchanges located abroad.

Consequently, crypto exchanges worldwide face a new age of global litigation related to incidents of fraud. From the English Court's perspective, this includes responding to claimant applications for disclosure orders seeking what is likely to be confidential information about the exchange's customer and the contents of the wallet. It will also involve defending High Court actions and dealing with notifications of worldwide freezing injunctions (where exchanges are asked to freeze the wallets of alleged fraudsters).

This article considers some of the legal challenges for crypto exchanges, created when they are asked to respond to applications for disclosure orders granted in the English Court, and how they might respond.

Types of disclosure order

Disclosure orders come in various forms but the most common are Bankers Trust Orders and Norwich Pharmacal Orders. The tests for each are distinct, with the former arguably being more stringent than the latter. However, both types of order are usually sought by victims, and served on crypto exchanges, because the victims know (or think they know) that an exchange holds evidence about the identity of a fraudster (or the whereabouts of the missing crypto) that, as victims, they do not have, and they believe that this information will support their investigation or case.

Bankers Trust Orders tend to be available only where there is a clear-cut case of fraud: that usually translates to a victim being able to say (1) on a clear case, that crypto belonging to them has passed through the exchange and (2) there is a real prospect that the information might lead to the location or preservation of the stolen crypto.

For Norwich Pharmacal relief to be obtained:

1. There must be a 'good arguable case' that a wrong has been committed by a wrongdoer;
2. The respondent against whom the order is sought must be "mixed up" in the wrongdoing, so as to have facilitated the wrongdoing; and
3. The order is needed to enable an action to be brought against the wrongdoer. The respondent to the application must be able, or likely to be able, to provide the information or documents necessary to enable the ultimate wrongdoer to be pursued.

In practice, the two orders can be applied for in combination and if the narrower Bankers Trust jurisdiction does not apply, the Court may be able to grant an order using Norwich Pharmacal relief. An exchange will usually be notified in advance by the victim that they intend to apply for a disclosure order (it is good practice to do so), but for various reasons that is not always the case, and quite often an exchange will find itself having to respond, often in short order, to demands for the provision of information.

The legal challenges and responding to them

Whilst complying with court orders is clearly essential, crypto exchanges need to be careful that they adopt an appropriate response. Some key considerations for a crypto exchange responding to an application for a disclosure order by a victim of fraud are set out below.

Have the necessary legal tests for obtaining a disclosure order been met?

Whilst a flexible remedy, the power to order third party disclosure is a powerful tool in the English Court's armoury, and the English Court will scrutinise each application carefully. The Norwich Pharmacal jurisdiction, for example, should not be used as a fishing expedition for wide ranging discovery and the gathering of evidence. Rather, it is strictly confined to necessary information (see Ramilos Trading Ltd v Buyanovsky [2016] EWHC 3175 (Comm)).

Consequently, exchanges should consider whether the stringent legal tests have been met, which will likely require expert legal advice. Exchanges may also question whether the scope of the draft order they are being asked to comply with is too broad, potentially because the provision of the information cannot actually be provided, or it simply does not relate to the factual matrix being described.

What is the underlying purpose of the disclosure order?

In circumstances where the identity of the fraudster cannot be found, it is not unrealistic that an exchange could potentially find itself the target of legal proceedings brought by the victim, in the same way banks and other financial institutions are targeted. In, D'Aloia v. (1) Persons Unknown (2) Binance Holdings Limited & Others [2022] EWHC 1723 (Ch), Mr Justice Trower acknowledged that cryptocurrency exchanges can hold misappropriated assets on constructive trust for defrauded investors.

It is too early to say whether victims of fraud will successfully pursue litigation against exchanges on this basis, and such claims are heavily fact-dependent. However, exchanges should nevertheless be mindful of the victim's motive for bringing the application, and whether it should be opposed: for example, a disclosure order should not be sought as a way of obtaining information in support of any proceedings to be brought against the exchange. Rather, the exchange against whom the order is sought must be "mixed up" in the wrongdoing, so as to have facilitated it, in order for a disclosure order to be granted.

Further, the information that is sought by the victim cannot normally be used other than for specified purposes (e.g., considering or commencing proceedings against the ultimate wrongdoer) without the permission of the Court. In I.F.T. S.A.L. Offshore v Barclays Bank Plc [2020] EWHC 3125 (Comm), IFT obtained permission to bring an application for pre-action disclosure and/or proceedings against Barclays Bank after obtaining information pursuant to a disclosure order which identified a potential claim against the Bank. Exchanges may find themselves having to respond to similar applications once information has been provided to the victim.

An exchange should obtain legal advice if it thinks an application is being brought on the wrong basis, for instance where it is ultimately in support of proceedings against the exchange, or if the provision of information is likely to compromise the position of the exchange.

Ultimately, should the exchange oppose the application for a disclosure order?

Adopting a neutral position and awaiting the outcome of the application, i.e., neither opposing or consenting to the application, may be the cheapest and most efficient response. However, just like banks and financial institutions are more traditionally required to do, exchanges will need to assess whether a neutral position can be adopted, particularly in circumstances where they may also owe duties of confidentiality to the holders of wallets. Disclosure orders are, however, quite often teamed with gagging orders which seek to prevent the exchange from "tipping off" the wallet holder or fraudster. A breach of the terms of a gagging order could have serious consequences for the exchange and care should be taken when navigating the provisions of such an order.

On a final note, provision should be made for the exchange to be compensated for its reasonable costs of providing the information, the level of which may well be significant depending on the scope and complexity of the request, and how time intensive the exercise becomes. A robust record of the time and costs incurred should be kept.