

“
PCB Byrne is a high-quality practice regularly instructed on high-profile fraud disputes, many of which are international. The firm also displays significant expertise in asset freezing and tracing and acts for both individual and corporate clients, often on cases that involve parallel criminal proceedings. It is particularly strong in matters concerning Europe, Asia, the Middle East and offshore jurisdictions.”

Chambers & Partners, 2023



In this Edition:

Page 2

Articles and Publications

Crypto - Special Feature

- Crypto assets and cybercrime

Page 3

PCB Byrne Answers FAQs

Page 8

Crypto Fraud

- The pump and dump
- Mis-sold cryptocurrency

Page 9

Disputes with Exchanges

- Exchanges wrongfully close out positions or prevent investors from closing out positions/ withdrawing crypto
- Exchanges' collapse

Page 10

PCB Byrne Hub

- The latest updates from the firm

Page 10

Recent speaking engagements

Future Speaking Engagements

Welcome to the Q1 2023 edition of the PCB Byrne Quarterly. This Quarterly series is the firm's insights of news and analysis of key market developments and court judgments in the last quarter, as well as insights from the firm.

This series will bring you up to speed with some of the key developments in commercial litigation, international arbitration, fraud, insolvency, investigations and more.

This edition includes a special round-up on disputes that might arise in relation to cryptocurrency.



Money laundering regulations and enforcement in the UK

Partner [Michael Potts](#) has written an article “Money laundering regulations and enforcement in the UK” for the 2023 February Issue of the *Financier Worldwide Magazine*. There is an obvious tension between the relevant authorities’ civil powers to fine for UK Money Laundering Regulations breaches and in some instances their parallel power to criminally prosecute for the same conduct.

To access the article, please go here. [↗](#)

The Police, Crime, Sentencing and Courts Act 2022: rejuvenating pre-charge bail

In this article, Associate [Sam Russell](#) considers the changes made to pre-charge bail by the Police, Crime, Sentencing and Courts Act 2022 and queries whether they will lead to improvements in the regime, especially for those suspected of alleged criminal offences.

The article is available here. [↗](#)

ICSID panel is not an international tribunal, New York District Court rules

Associate [Yana Ahlden](#) examines the interaction between international arbitration and American disclosure law considering the recent decision by US District Court for the Southern District of New York in *Re Webuild* and the US Supreme Court in *ZF Automotive*.

Please read the full article here. [↗](#)

Al Mana Lifestyle Trading LLC and others v United Fidelity Insurance Company PSC and others

[2023] EWCA Civ 61

Associate [Joshua Oxley](#) examines the recent case of *Al Mana Lifestyle Trading LLC and others v United Fidelity Insurance Company PSC and others* [2023] EWCA Civ 61. In this case, here the Court of Appeal allowed the defendants’ appeal by deciding that an “Applicable Law and Jurisdiction” clause in several insurance policies did not confer the English court jurisdiction.

Please read the full article here. [↗](#)

LMN v Bitflyer Holdings Inc

[2022] EWHC 2954(Comm)

Senior Associate [Tom McKernan](#) considers the status of the new service out gateway in light of the recent case of *LMN v Bitflyer Holdings Inc* [2022] EWHC 2954.

Please read the full article here. [↗](#)



Crypto assets and cybercrime

- The rise of cryptocurrency “crypto” assets and decentralised finance presents unique risks for businesses and individuals operating in the digital economy, as well as being an extremely amenable new asset class for traditional frauds.
- By their nature, fintech disputes are often highly technical and factually complex. They also frequently require the determination of novel legal issues and often give rise to regulatory issues or allegations of criminality.
- Crypto assets in particular present unique risks to litigants. Due to their decentralised nature they can be transferred between jurisdictions to jurisdiction instantaneously and relatively anonymously, often without any oversight by the crypto asset service providers involved in the transfers.
- This means the successful recovery of crypto assets often involves the co-operation of specialist lawyers, technical investigators, and overseas counsel.
- Realising you have been the victim of a fraud can be an extremely stressful and confusing experience. The actions you take following such an event can have a significant impact on whether you are ultimately able to recover your assets. While each case is unique, most victims of crypto fraud share common concerns and questions upon realising what has occurred – we have endeavoured to answer these below.

PCB Byrne Answers Frequently Asked Questions¹



Questions and Answers:

1 How was my crypto taken – have I been hacked?

There are many ways that people can get their hands on your crypto. They can trick you into handing it over to them (this is often referred to as [authorised push payment fraud](#)), they can hack into your computer or phone and obtain all of the relevant details to misappropriate your crypto, or they can take it directly from the exchange (among others). How your crypto was taken is certainly important, but what you do next is crucial.

2 I believe I am a victim of a crypto fraud – what should I do?

First, you should act quickly because delay allows the fraudster(s) time to conceal the original source of the crypto and may make it more difficult to obtain helpful orders from the court (such as freezing orders).

Due to the pace with which this area of technology and the law evolves, you should also consider seeking the advice of specialist investigators and lawyers who deal with these issues on a day-to-day basis as well as reporting the fraud to the relevant exchanges and/or the police. (This is elaborated on further below).

¹ For the avoidance of doubt, the content below is not legal advice and cannot be relied on as such. Each case is fact specific and requires bespoke advice.



3 I have only lost a modest amount of crypto – can I still go after it?

If you have been defrauded out of a modest amount of crypto it may be uneconomic to pursue the fraudster(s). However, there are many factors to consider when determining whether such a pursuit is commercially viable, including, whether the identity of the fraudster(s) is known; their location; the location of the crypto; and whether there are other victims of the same fraud who might be able to share the cost, among others. If there are many victims and the total amount lost is significant, litigation funding may be a viable option (more information on litigation funding [here](#)). [↗](#)

4 Where could my crypto have gone? Can I trace it?

Transactions for almost all commonly traded cryptocurrencies are recorded on a publicly available ledger (e.g. the blockchain). Therefore, there is a good chance that your crypto is traceable. This is important as it can maximise your chances of recovery. Fraudsters may employ techniques (for example, crypto tumblers) to conceal where crypto has gone – however, we work with experts with specialist technology who are able to trace this information across the ledger (or ledgers). What's important is that the quicker a tracing exercise can be undertaken, the more likely it is to succeed.

Even if your crypto proves to be untraceable, there may still be avenues of recovery available.

5 I don't really know how I have been defrauded, is that an issue?

Not necessarily - most victims of fraud do not know what has happened at the outset and the English courts have developed various mechanisms to assist people in such a position.

In particular, where traceable crypto assets have been identified, orders can be obtained against 'innocent' third parties, who may have played no role in the fraud but nonetheless hold relevant information such as crypto exchanges, which may well hold useful Know Your Client/identity verification documents. Since 1 October 2022, a new gateway has been added to the Civil Procedure Rules and it is now more straightforward to obtain information from parties outside of the English jurisdiction (for more information please see [this article](#)). [↗](#)

6 Can I get my crypto back? If so, how?

It can be possible to get your crypto back. If your misappropriated crypto can be traced to an exchange, one option is to notify the exchange that they are holding stolen crypto and ask them to hold it while you establish your claim to ownership. In such a scenario, the exchange may even return your crypto voluntarily.

In cases where your losses are larger, you may be able to obtain a freezing order, which orders the defendant not to deal with the crypto or his/her assets pending recovery via court proceedings. If you can pinpoint or trace your crypto into a particular wallet, you may be able to obtain an asset preservation order which locks up this particular crypto rather than the general assets held by a defendant. Freezing orders can also be obtained against third parties (for example, crypto exchanges or third parties which have received the proceeds of the crypto) as well as against the party who initially stole the crypto.

Freezing order applications may be made without informing the other party and they can be heard in private by the court. This prevents tipping off the fraudsters. They can even be made against assets worldwide, meaning they can be sought against assets moved overseas.

The courts have held that freezing injunctions may be obtained against 'persons unknown'. This means, crucially, that in order to obtain asset freezing relief, it is not necessary to identify the fraudster or their intermediary – only property that represents the proceeds of the fraud (*AA v Persons Unknown* ([2019] EWHC 3556 (Comm))).

Any person who knowingly assists in the breach of a freezing order can be held in contempt of court, which may result in them being sent to prison. There is a strong incentive for third parties (for example, exchanges) to ensure that a defendant does not breach a freezing order, and it is therefore often advisable to serve the freezing order on appropriate third parties to ensure compliance.

In cases where there is a concern that a defendant will disobey a freezing order, the English courts have powers to have the assets in question transferred to a third party and held in escrow whilst the claims are pending. So, in an appropriate case, a claimant could seek an order requiring the crypto to be transferred to a secure wallet (which is not under the control of the alleged fraudster), to give an extra level of comfort.

A claimant may also seek to bring substantive claims against parties other than the fraudster, which require those parties to return the crypto. Since misappropriated crypto is often transferred between multiple wallets and exchanges, and through multiple different people/entities, tracing the path of your crypto might identify third parties who were involved in your fraud or received proceeds from it – there might be claims that could be made against them as well or instead.





7 I am based overseas, can I still file a claim in the English courts?

The fact that you do not live in England does not mean you cannot bring a claim here. Whether you can or not depends on the facts of your case. In all cases with an international element, determining the most appropriate jurisdiction to litigate in needs to be resolved.

The English court might have jurisdiction over a dispute in various cases – for example:

- If there is a relevant contract subject to the jurisdiction of the English courts;
- If damage has been suffered in England;
- If the defendant is domiciled in England; and
- If there is an “anchor” defendant (e.g. exchange) that the English courts have jurisdiction over, then the courts can add additional defendants that are necessary or proper parties to that litigation.

Therefore, overseas claimants can file claims in the English courts – as long as the facts of their case permit them to do so.

8 What happens if the relevant fraudster or exchange(s) is not based in England & Wales?

Where a defendant is located outside of the jurisdiction, a claimant is usually required to seek the court’s permission before serving proceedings on the defendant(s).

To obtain this permission, a claimant must show:

- The claim has a reasonable prospect of success; and
- The claim falls within one of a number of categories or jurisdictional “gateways” (as listed in the Civil Procedure Rules); and
- England is the proper place to bring the claim.

By way of example, claims in tort (e.g. deceit) can be brought here if a claimant has suffered loss or damage in England and the acts giving rise to that loss or damage occurred in England.

The elements above were considered in the digital fraud case of *Ion Science v Persons Unknown* [2020] (unreported). There, the victim of the ‘Initial Coin Offering’ fraud was located in England and purchased crypto using funds in an English bank account. The victim was induced to make the investment as a result of representations made to him by the defendants in England. These facts were sufficient to establish that there was a serious issue to be tried, that gateways detailed in the Civil Procedure Rules applied, and that England was the proper forum for the dispute.

Additionally, in June 2022 the English High court granted an applicant’s request to serve a legal notice via an NFT². The notice was embedded into the NFT which was sent to the digital wallet controlled by the anonymous defendant that had misappropriated the crypto at the heart of the dispute. This is a novel way to serve a party to proceedings and illustrates the English court’s adaptability in this developing area of law.

² *D’Aloia v Person Unknown & Ors* [2022] EWHC 1723 (Ch) (24 June 2022)

9 What do I do if the fraudster won't hand over their password on a crypto wallet?

If you have an order of the court compelling someone to give you a password/encryption key, and they do not, they can be held to be in contempt of court.

The law of contempt allows the court to hand down fines, sequester assets or imprison people so that its orders are obeyed. Such orders are generally more effective when the defendant has assets within the United Kingdom or wishes to travel here.

10 Who do I report this to - should I report my matter to my exchange, the police or both?

Reporting a fraud to your exchange is a sensible step. They may be able to provide information that may be helpful and they also may be able to plug any gaps in their security to prevent any further loss.

Reporting potential frauds to the Police is a sensible step. There is an impetus in international law enforcement towards limiting the impact of crypto crime, and depending on the facts of your case, law enforcement agencies may be able to provide helpful input. Additionally, reporting your case to [Action Fraud](#) is also recommended.

Where case studies are included, results achieved do not guarantee similar outcomes for other clients.

11 Are my crypto deposits protected?

Some deposits with banks, building societies and credit unions are covered up to the value of £85,000 by the Financial Services Compensation Scheme ("FSCS") (which is ultimately accountable to the Financial Conduct Authority ("FCA")). However, as crypto is currently not regulated by the FCA, it is not covered by FSCS compensations scheme.

12 How common is crypto fraud?

Crypto fraud is very common. Even the most sophisticated individuals can, and have, been defrauded. In fact, since the start of 2021, more than 46,000 people have reported losing over \$1 billion in cryptocurrency to scams (for more information on this topic please see this [article](#)). 



If any of your questions haven't been answered, please contact our specialists who are able to assist you with any further queries:



CHARLOTTE BHANIA
Partner
cbhanja@pcb-byrne.com



TOM MCKERNAN
Senior Associate
tmckernan@pcb-byrne.com



JONOTHAN GOULD
Senior Associate
jgould@pcb-byrne.com

In a previous section we answered various questions a victim of crypto fraud may have. And while many crypto frauds are as innovative as the underlying technology, investors should also be alive to the fact that frauds which take place under the traditional finance commonly involves cryptocurrency issue.

[These are discussed below](#)

The pump and dump

In simple terms, it is an orchestrated attempt to boost the value of an asset on the basis of misleading, false or outlandish claims. The perpetrators of the scheme take a position in the relevant asset, make public statement to inflate its value and then sell it at its height, leaving the retail investors “holding the bag”. In the traditional finance system such a scheme was typically perpetrated by salespeople on a trading floor. In the crypto sphere, it is more likely to be committed by influencers on Instagram, Twitter or TikTok.

Unfortunately, crypto is particularly amenable to such a scheme due to its inherently borderless nature, opacity and limited regulation. Indeed, [a 2018 study \(updated on 21 February 2023\)](#) identified 3,412 pump and dump announcements in respect of crypto on centralised exchanges over a 16-month period. Given the wide variety of ways that the schemes can manifest, it is not possible to provide general advice. However, if you think you have been the victim of the pump and dump scheme, various avenues of redress may be available (depending on the facts of your case).

Mis-sold cryptocurrency

This arises where characteristics of a financial product are not properly explained, or the product is not applicable to the relevant consumer.

In the context of crypto, such claims are likely to be claims for misrepresentation. That is, someone made a false statement to you about a key fact that induced you to enter a contract – in this case to buy crypto. There are various types of misrepresentation; innocent, negligent and fraudulent.

A fraudulent misrepresentation arises when party A knowingly or recklessly makes a false statement to party B. A negligent misrepresentation occurs when a party carelessly makes a misrepresentation to another, and they owe that party a duty of care. And an innocent misrepresentation is a misrepresentation that is neither fraudulent or negligent.

If you have been induced to buy crypto as a result of a misrepresentation you can take the misrepresenting party to court and seek rescission and/or damages. Rescission means a contract is set aside and the parties are put back in the position they were before the contract was made. So if a crypto salesman has told you that prices will definitely only go up and your crypto will yield 20%, and that turns out not to be true, you may have a misrepresentation claim against them, their company, or both.



Exchanges wrongfully close out positions or prevent investors from closing out positions/withdrawing crypto

There are various ways to invest in, or get exposure to, crypto. One straightforward way is to just buy a crypto asset, say Dogecoin. If the price goes up, you make money (and vice versa). However, a slightly more sophisticated way to invest is to trade “on margin”. This just means that you are borrowing currency from a brokerage firm to carry out trades.

Such an arrangement typically works with the investor having a margin requirement that they must maintain (for example, this could be 50%). In such a situation, the investor can purchase £100,000 worth of Dogecoin by depositing only £50,000 of their own money into their margin account.³

The brokerage typically holds the purchased asset as collateral so that if the price drops to £75,000 for example, they can sell the Dogecoin and not lose their £50,000.

When the price of an asset bought on margin falls, brokerages typically make “margin calls” to investors requiring them to deposit additional funds into their margin accounts so that the brokerage does not need to sell the asset. However, given the extreme volatility of certain crypto assets it is possible that brokerages may liquidate positions before a client has had the time to respond to a margin call. Such forced liquidations can be a source of disagreement between an investor and a brokerage – particularly in volatile assets such as crypto. Whether the broker has acted lawfully or not in liquidating the crypto will primarily turn on the interpretation of the contract between the client and the brokerage.

³ Such an arrangement is beneficial for the brokerage as they can make a return on the funds they lend. It can also be beneficial for the investor as gains are magnified. Unfortunately, the same is true of losses.

⁴ However, in the UK there is the Financial Services Compensation Scheme which may cover your losses up to a value of £85,000.

⁵ In *Ruscoe v Cryptopia Ltd (in Liq)* [2020] NZHC 728 the High Court of New Zealand held the exchange (in liquidation) to be a trustee.

⁶ This risk is different from a ponzi scheme (where funds from later investors are used to pay “returns” for earlier investors) or “fake” initial coin offerings where the particular crypto may not even exist. In both instances the fraudster(s) are essentially taking your crypto for themselves.

Exchanges’ collapse

When you deposit cash at a bank, you do not actually own the cash in your account. Rather, the bank owes you a debt equal to the size of your deposit. This is important as if the bank goes insolvent, you may not get all of your money back.⁴

As there are many different crypto exchanges in many different countries, the way your particular crypto assets are classified is currently up for debate and will be largely determined by

- The terms and conditions you agreed to as a customer; and
- The way the exchange has actually dealt with your cryptocurrency.

At one end of the spectrum the exchange may provide a digital “box” that they place your asset, and only your asset in, with you retaining legal and beneficial ownership. While at the other end of the spectrum the exchange may take ownership of the asset and you, as the depositor, will have a debt claim against them to give you that asset back. There are also exchanges that provide services somewhere between the two. One example is that the exchange may own the asset, but it may also be held to be a trustee – such that it owes depositors fiduciary duties.⁵

As in the situation with a traditional bank, the answer to how your assets are held is important if the exchange collapses.⁶ If the assets are segregated, and you maintain ownership, you should get your assets back. However, if the assets are owned by the exchange, you may only receive a fraction of the value of your assets back if the exchange is placed in receivership or liquidation. This is because you will very likely be an unsecured creditor.

The volatility in crypto markets experienced in 2022 resulted in the:

- Bankruptcy of [FTX](#);
- Bankruptcy of [BLOCKFI](#);
- Restructuring of [Voyager](#);
- Bankruptcy of [Celsius Network](#); and
- Liquidation of [Three Arrows Capital](#).

Considering how your crypto assets are held, and thus whether and how much you can recover, is more important than ever.

THE HUB The latest updates from the Firm



In January and February 2023, we welcomed new members to our PCB Byrne litigation team: Associates Yana Ahlden and Katie McKernan.

Yana specialises in high-value, complex commercial disputes, and arbitrations. She has experience with shareholder and contractual disputes, as well as insolvency proceedings. Yana is also a member of the London Very Young Arbitrators Practitioners and the LCIA Young International Arbitration Group. She speaks German, Spanish and Portuguese and is learning French.

Katie is a solicitor qualified in Scotland with experience in complex disputes, arbitrations and professional regulation across a wide variety of sectors and disciplines, including contract, property, healthcare and competition. She has worked on matters involving both Scottish and English law and is currently working towards dual qualification in England and Wales.

RECENT SPEAKING ENGAGEMENTS

- Senior Associate [Jonothan Gould](#) delivered a presentation on collective action against Crypto Exchanges at the Thought Leaders 4 Disputes Conference in London on **19 October 2022**.
- On **23 November 2022** our Managing Partner [Sara Teasdale](#) joined a formidable line up of experts to share her experience and advice as part of the launch of [Networking Nuance](#), the brainchild of two partners Kate McMahon and Tamlyn Edmonds at Edmonds Marshall McMahon LLP. Sara was delighted to be interviewed for Networking Nuance's new 9-week e-mentoring programme for female lawyers and professionals. The programme focuses on helping women in law and other professions to fast track their rainmaking skills with ultimate aim of re-balancing leadership in law firms and companies.
- Partner [Nick Ractliff](#) was a member of a panel speaking on Shareholders Claims at the Thought Leaders 4 Disputes Financial Institutions Litigation Conference on **19 January 2023**.
- Senior Partner [Anthony Riem](#) and Senior Associate [Catherine Eason](#) were in Dublin for the FIRE Starters Global Summit "The Next Gen of Asset Recovery" on **22 - 24 February 2023**. As part of the Thursday programme, Catherine chaired the afternoon session "FIRE Starters Committee Welcome Back" with Sam Goodman from 20 Essex. Anthony spoke at the morning workshop session "Negotiation: tips, traps and tactics" and participated as a panellist in "The Big Fat Quiz of the Year" on Thursday afternoon. Please see the full agenda for the Summit at: <https://thoughtleaders4.com/fire/fire-event/fire-starters-global-summit/agenda>
- Partner [Nicola Boulton](#) was in Geneva at the [C5 Group Inc. Fraud, Asset Tracing & Recovery Conference](#) on **16 - 17 March 2023** and spoke at the panel session "As the World of Fraud Turns: A Global Recap of the Most Pressing Challenges in Fraud and Asset Recovery". The panel provided an international perspective on the most significant challenges experienced in fraud and asset recovery matters, including examining the different approaches taken on disclosure and discovery in civil and common law jurisdictions.

FUTURE SPEAKING ENGAGEMENTS

- Partner [Nicola Boulton](#) will be a guest speaker at the live event "How to succeed in Commercial Law: All you need to know" for female barristers and lawyers on **22 March 2023**. The first episode of [Networking Nuance's](#) e-mentor programme to help women rain-make and then hearing from those who have excelled in commercial litigation will be broadcasted.



Civil Fraud and Commercial Dispute Services

Asset Recovery and Enforcement Civil Fraud

Commercial Litigation

Insolvency and Restructuring

International Arbitration

Business Crime and Regulatory Services

Asset Seizure and Forfeiture

Corporate and Financial Crime

Corporate Investigations

Regulatory and Disciplinary

Serious and General Crime

PCB BYRNE LLP

1 Plough Place

London EC4A 1DE

www.pcb-byrne.com



Follow us on LinkedIn

#extraordinaryproblemsolvers

PCB Byrne Quarterly Newsletter is published by PCB Byrne LLP as a news reporting and briefing service for general guidance only and should not be used for any other purpose. It does not constitute and should not be relied upon as legal advice.

Where case studies are included, results achieved do not guarantee similar outcomes for other clients.

CONTACTS

Charlotte Bhanja
cbhanja@pcb-byrne.com

Nicola Boulton
nboulton@pcb-byrne.com

Emma Brooks
ebrooks@pcb-byrne.com

Uliana Cooke
ucooke@pcb-byrne.com

Ben Davies
bdavies@pcb-byrne.com

Matthew Frankland
mfrankland@pcb-byrne.com

Trevor Mascarenhas
tmascarenhas@pcb-byrne.com

Michael Potts
mpotts@pcb-byrne.com

Nick Ractliff
nractliff@pcb-byrne.com

Anthony Riem
ariem@pcb-byrne.com

Elizabeth Seborg
eseborg@pcb-byrne.com

Sara Teasdale
steasdale@pcb-byrne.com