ThoughtLeaders4

navigate the legal maze

CRYPTO INSIGHT 2022

EDITOR'S COMMENT

The global cryptocurrency market size was valued at US$1.49 billion in 2020 and is projected to reach US$4.94 billion by 2030. Developing countries have started using digital currency as a financial exchange medium and the increasing popularity of digital assets such as Bitcoin (despite the recent selling pressures) and NFTs is likely to further drive market growth.

However, with the growth of digital assets comes a parallel growth in fraud. Some US$8.6 billion in cryptoassets is estimated to have been laundered in 2021 alone and it is likely that financial crimes will accelerate in direct proportion to the use of cryptocurrency.

As a result, cryptocurrency disputes are on the rise. Although few countries have a regulatory framework in place to protect such assets, many jurisdictions, including the UK and the US, regard crypto assets as property which has led to a number of complex legal challenges.

In this special Insight, we examine the various areas of disputes where crypto is involved, including fraud and asset recovery; HNW divorce; Private Client services; and dispute resolution. The good news is that while crypto fraud is on the increase, so too are the systems developed to trace these formerly untraceable assets.

As our Guest Editor, international forensic investigator Burke Files, says: "It is all blockchain and very traceable when you have found the entry point".

So what measures can companies take to deal with the risks involved? In his article "Shutting Down the Virtual Laundromat: Cryptoassets and UK Money Laundering Law", James Potts of 3VB outlines the main money laundering risks and the available anti-money laundering solutions.

Lizzie Williams of Harbottle offers a private investor's survival guide to crypto in disputes and warns that there is no substitute for swotting up on what you are investing in and seeking legal and financial advice beforehand. This warning of "Be Prepared" is echoed by Carmel King of Grant Thornton who offers essential considerations for crypto disputes.

Alarmingly, in the past year, law firms, barristers' chambers and legal professional bodies have found themselves to be the target of cyber-attacks designed to extract ransom payments from legal professionals. Darragh Connell of Maitland Chambers explains the legal remedies that can be actioned when this occurs.

Now that crypto assets are regarded as property, they increasingly feature in HNW divorce proceedings. Fortunately, according to Katharine Landells from Withers, hiding assets or obstructing their recovery is no longer as easy as it was and case law is now being made in relation to the freezing of NFTs and cryptocurrency.

What is clear from the input of our thought leaders is that while the courts have shown that they are willing to offer assistance when possible, the easiest way of resolving a crypto dispute is through due diligence and wise counsel, to prevent it from happening in the first place.

Georgina Hatch
Consulting Editor

PAGE OF CONTENTS

THE 5Ps OF ASSET TRACING IN THE DeFi WORLD

Authored by:
L Burke Files
President
Financial Examinations & Evaluations Inc.

I have been a forensic investigator for over 30 years and I have to say that the last fistful of years have been some of the most interesting as cryptocurrency has gone mainstream. The good news is it is all blockchain and very traceable when you have found the entry point.

In 2016, a young American married couple, Ilya Lichtenstein and his wife, Heather Morgan, stole 199,754 bitcoins from Bitfinex's platform. In 2022, the US Department of Justice, following the money, executed search warrants on their online accounts, located their wallet and the necessary access credentials, and recovered 94,000 bitcoins. This is about US$3.6 billion. It was difficult, complex, and meticulous work.

Your response may be "Yeah, but we do not have those resources." True, but we have something law enforcement does not have. We have the ability to act more freely in our research and recovery because we are not mounting a criminal case. My joy is a broke fraudster, after recovery efforts, looking for a public defender to address the criminal complaint.

By the time forensic investigators are engaged, there is already a good idea of how assets were pillaged, not where they went. While we'll know the path out, we have to discover how the assets were transmogrified and spirited away.

In the past, we looked for entities, bank and brokerage accounts, and property. Finance was fairly centralised, and it was harder to hide but easier to find. Today, with digital assets, it is easier to hide and harder to find. No matter the environment, I find the 5 Ps: Pillage, Path, Pail, Play, Pregnant, to be a reliable process for finding assets for a recovery.

Paths have trailheads and trail ends. The Paths lead to Pails. To discover what Paths were taken, you have to look for maps. The maps are found on computers, phone usage, and emails as well as purchases from Amazon, eBay, and other websites. When a fraudster is looking to hide money, they educate themselves. No-one comes to asset protection without a maven urging them on and a guide to illuminate the path. Look to the friends of the fraudster and those who might be guides.

Pails are used to hold assets. A Pail can be property, a trust, a captive insurance company, a specialty insurance policy, or even just cash sitting in a bank under the name of an entity they control. However, with decentralised finance (DeFi), they must acquaint themselves with how DeFi can be used to hide assets. Using US$500K of crypto to buy an NFT is beautiful. Especially if the fraudster also controls or is the seller of the NFT. The transaction is meant to look like a dead-end when in fact, it is an artful money laundering technique.

Play is the purpose of the fraud. The entire idea of the crime is to enjoy the fruits of one's conniving labours. Where does the fraudster travel, how do they travel, who are the travel companions, what is purchased, and for whom? My experience is that fraudsters make more mistakes when they commence enjoying the fruits of their frauds. Renting jets and villas through an agent and using their crypto for payment has proved to be a good way to track them.

Pregnant is a term of art to describe the future condition for all of those who assist the fraudster. If it were not for the help of friends and professionals, the little old ladies in white tennis shoes would still have their retirement savings. Therefore, friends and professionals, the recovery team is going to use its best efforts to make you jointly and severally liable for the losses.

This is just a brief expose of the process. There is much more. But one thing's for sure – as the popularity of virtual assets grows, fraudsters will continue to find more cloak-and-dagger ways to hide their nefarious activities and disputes will continue to challenge the best legal minds.

Burke Files is an international financial investigator and due diligence expert who has run cases in over 130 countries and has visited over 100 countries, tackling investigations running from a few hundred thousand dollars to over 20 billion. He is the author of the award-winning book Due Diligence For The Financial Professional 2nd Edition along with five other books.

Brown Rudnick's International Litigation Team based in England, France and the US has extensive experience in pursuing wrongdoers around the World, including all of the major offshore centres and includes former US federal prosecutors from the Department of Justice, Securities and Exchange Commission, the Department of Defense and the UK's FCA, as well as lawyers with decades of experience in anti-money laundering/anti-corruption investigations throughout the world.

- Our lawyers are experienced in acting for States and public bodies with the ability to take on large, global institutions including many banks.
- We have a proven track record of successful recovery.
- We act for both claimants and defendants in civil fraud proceedings, giving us a detailed understanding of the tactics deployed on both sides and enabling us to strategise both claims and defences in civil fraud proceedings effectively.

brownrudnick

www.brownrudnick.com

ATTORNEY ADVERTISING

ARBITRATING BLOCKCHAIN AND SMART CONTRACT DISPUTES: THE SMARTER SOLUTION?

Authored by:
Jessica Lee
Associate
Brown Rudnick

Blockchain functionality is rapidly expanding through the advent of smart contracts, essentially self-executing code built on the blockchain with uses ranging from creating currencies and storing data to enabling users to engage in financial borrowing and saving through DeFi (decentralised finance) platforms. The attraction of blockchain technology for many enthusiasts is its speed and efficiency, its immutability, pseudonymity, and its decentralised nature. So, when it comes to resolving blockchain and smart contract disputes, users are likely to seek out methods of dispute resolution which stay true to the ethos of blockchain technology and enable disputes to be resolved quickly while maintaining consumer autonomy and financial privacy.

Arbitration is therefore likely to be an appealing mechanism for settling disputes arising on the blockchain. But in the blockchain space, "arbitration" is a broad term, capturing both "off-chain" arbitration (i.e., traditional arbitration using existing commercial arbitral rules or dedicated blockchain rules such as those offered by JAMS) and "on-chain" arbitration using smart contracts to automate all or some of the arbitral process.

Off-Chain arbitration: the role of existing commercial arbitral rules in blockchain disputes

A number of crypto exchanges and NFT marketplaces already incorporate arbitration agreements into their standard terms of use. For example, popular crypto exchange, Binance, contains an arbitration agreement in its terms and conditions which provides for all disputes to be referred to arbitration administered by the Hong Kong International Arbitration Centre. The enforceability of an arbitration agreement contained in the standard terms of use of US-based NFT marketplace, Nifty Gateway, was also recently the subject of a dispute before the English court. There, the English court stayed the court proceedings in favour of JAMS arbitration proceedings in New York, concluding that arbitration was the proper forum for the dispute.

It is clear that existing commercial arbitral rules can and do already play a role in resolving blockchain disputes, and many of the pros and cons of the arbitration vs litigation argument similarly apply in the case of blockchain disputes. Particular advantages of off-chain arbitration to blockchain users include:

- Enforceability: Given the borderless nature of blockchain technology and international participation in crypto asset markets, enforceability is likely to be a key consideration. Arbitration agreements and arbitral awards are widely enforceable transnationally through the New York Convention in over 150 contracting states. This is likely to be a particular consideration for UK claimants following Brexit which has left the UK enforcement position in a bit of a mess, with enforcement of English court judgments at the mercy of the domestic laws of the foreign state where enforcement is sought, and foreign judgments having to be enforced in England applying common law rules.
- Expert arbitrators: Parties are able to choose the constitution of the arbitral tribunal and may specify or agree that individuals with a particular expertise are selected, such as those with coding or developing expertise.
- Flexibility: A significant advantage of arbitration is the ability to tailor the procedure to the parties' specific needs. Given the rapid innovation in the cryptosphere and novelty of the technology involved, the flexibility offered by arbitration is likely to be a key attraction in resolving blockchain disputes.
- Confidentiality: One of the appeals of the blockchain is that parties can transact with each other anonymously and blockchain users may therefore prefer to have their disputes dealt with by way of a confidential arbitration in order to maintain this feature of privacy.

Parties incorporating an arbitration agreement into their contractual relationship should pay particular attention to drafting. Key issues requiring consideration include:

- The scope of the arbitration agreement and the nature of disputes which are to be referred to arbitration under the agreement.
- The composition of the Tribunal and any particular expertise required.
- The seat and applicable law which should be expressly dealt with so as to avoid disputes over jurisdiction. This is likely to be a key area of challenge given the decentralised manner in which the blockchain operates.
- What arbitral rules or procedures the parties wish to adopt. For example, are the existing commercial arbitral rules offered by bodies such as the London Court of International Arbitration (LCIA) suitable or do the parties want to incorporate a set of blockchain focused arbitral rules such as the UK's recently published Digital Dispute Resolution rules (DDR) or the JAMS draft smart contract rules?

The UK Digital Dispute Resolution rules: an "on-chain" offering in an off-chain procedure

The DDR was published in April 2021 and designed to enable the rapid resolution of blockchain and crypto disputes by offering users a straightforward procedural framework to facilitate arbitration or expert determination of disputes.

A unique feature of the DDR is that the Tribunal has the power to effect decisions on-chain, including to operate, modify, sign or cancel any digital asset and to direct any interested party to do any of those things. This does, however, depend on parties willingly disclosing their private key to the Tribunal which is likely to be met with significant resistance in practice as possession of the private key enables one to freely deal with all of the assets in the wallet and disclosure therefore presents a significant security risk. One possibility to compel a party to disclose its private key might be to apply to court for an order under s.44 Arbitration Act 1996.

The DDR has a number of other novel features worth noting which are likely to appeal to blockchain participants, including:

- The framework provides for the recognition of on-chain dispute resolution processes (e.g., coding in a smart contract which self-executes if specific conditions are met). As a result, where a digital asset incorporates the DDR and an on-chain dispute resolution process, the DDR provides that the on-chain process is binding. Only disputes not captured by the on-chain process are referred to arbitration.
- Like traditional arbitration agreements, the DDR is incorporated by agreement between the parties. The DDR uniquely provides for electronic and encoded incorporation.
- The commencement and resolution of disputes under the DDR are designed to be straightforward and efficient, requiring decisions to be issued within 30 days from the date of the appointment of the Tribunal.
- There is little scope for parties to drag their feet and delay proceedings by disputing the constitution of the Tribunal as while the relevant appointment body, the Society for Computers and Law (SCL) must have regard to the parties' specified or agreed preferences as to the number, identity or qualifications of arbitrators, the SCL is not bound by them.
- The Tribunal has absolute discretion over a number of matters including the procedure to be adopted (having regard to the particular circumstances of the case, to available technologies and to the need to resolve dispute expeditiously and without unnecessary cost); whether to admit any evidence and if so, in what form; and the form of submissions. Notably, there is no absolute right to an oral hearing.
- Reflecting the position that the parties are likely to have transacted anonymously on the blockchain in the first place, the DDR provides for optional anonymity so that parties must identify themselves to the Tribunal but not necessarily to each other.
- There is no right to appeal on a point of law, which in practice means that an appeal may only be brought under s68 Arbitration Act 1996 on the basis of a serious irregularity, but conversely offers greater finality in the process.

On-chain arbitration solutions

On-chain arbitration includes a wide spectrum of possibilities. including self-executing code contained within smart contracts (designed to execute and enforce on satisfaction of certain conditions) to decentralised peer-to-peer justice systems where a consensus of blockchain users stake crypto to vote on the outcome of a dispute, such as Kleros.

There are now a number of platforms offering "on-chain" arbitration services (e.g., Juris, Confideal, Mattereum and CodeLegit to name a few). Many share common features including:

- A requirement for the parties to opt-in to the platform by incorporating specific code into their contract which automatically refers a dispute to resolution by the platform.
- Parties to select the number and/or expertise of arbitrators or jurors at the outset.
- An automatic freezing mechanism which pauses or freezes the smart contract once a dispute has been initiated.
- An on-chain enforcement process enabling a decision to be executed immediately on the blockchain without needing to seek any further enforcement measures.

So, does arbitration offer a smarter solution to resolving blockchain and smart contract disputes?

Giving the typical lawyer answer: it depends. On-chain arbitration platforms may offer a quick and cost-efficient technological option to resolving disputes. However, there are issues which have not yet been tested, such as whether such decisions will ultimately be upheld and enforced by local courts, which may leave on-chain decisions open to further challenge. There are also other potential problems, including the lack of experience of arbitrators or impartiality of jurors (who may be financially incentivised, depending on the model) and limitations on providing supportive evidence or documents.

Further, in most arbitral processes both off and on-chain, there is limited scope for seeking orders against non-parties or obtaining interim remedies such as freezing or proprietary injunctions pending resolution of the dispute. These may well be important considerations as cryptoassets may be held by non-parties, such as exchanges, and parties may be able to defeat enforcement by instantaneously transferring away cryptoassets at the click of a mouse.

In light of the above, parties should consider their requirements at the outset to determine which method of dispute resolution from the wide array of options available is most suitable to their relationship and to address their concerns.

Three Verulam Buildings Barristers

Cyber Fraud & Cryptocurrency at 3VB

3VB is at the cutting edge of cases involving cyber fraud, cryptoassets and blockchain disputes worldwide.

Members of Chambers advise on all aspects of cyber fraud and cryptocurrency, including litigation and arbitration; freezing injunctions (including against "Persons Unknown"); Norwich Pharmacal/Bankers Trust disclosure orders tracing the proceeds of fraud; blockchain tracing; compliance, anti-money laundering and counter-terrorist financing; regulatory enforcement proceedings (including by the Financial Conduct Authority); sanctions; smart contracts; and securities transactions.

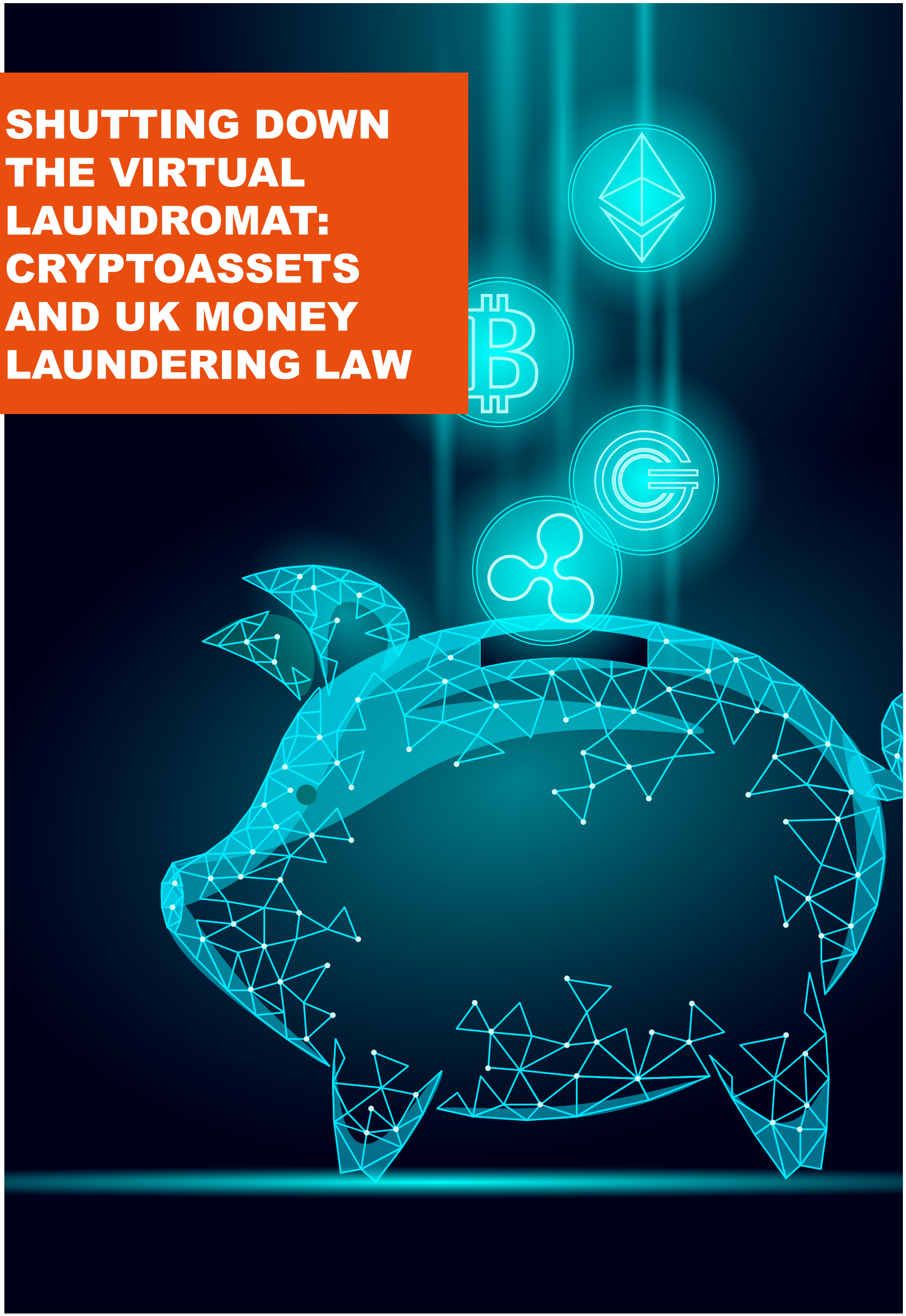
Highlights of 3VB's recent and ongoing work in this area include:

- A major independent review of the money laundering and terrorist financing systems and controls of one of the UK's largest cryptoasset exchanges, seeking registration with the Financial Conduct Authority under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.
- The first cryptoasset case before the Upper Tribunal, concerning crypto ATMs: Gidiplus Ltd v FCA [2022] UKUT 00043 (TCC).
- Obtaining Norwich Pharmacal disclosure orders against a cryptoasset exchange in Australia in aid of tracing funds laundered as part of an international banking fraud in Malaysia and other jurisdictions.
- The first Dubai International Financial Centre (DIFC) claim to consider the legal status of cryptocurrency.
- Members of Chambers regularly act for and advise clients on cyber and cryptocurrency disputes in overseas jurisdictions.

3 Verulam Buildings, Gray's Inn, London, WC1R 5NT
T. 020 7831 8441 W. chambers@3vb.com

Please follow us on LinkedIn and Twitter

SHUTTING DOWN THE VIRTUAL LAUNDROMAT: CRYPTOASSETS AND UK MONEY LAUNDERING LAW



Authored by:
James Potts
Barrister
3VB

In a virtual world where over US$500 million in cryptocurrency can be hacked and laundered at the click of a mouse,[1] and where some US$8.6 billion in cryptoassets is estimated to have been laundered in 2021 alone,[2] how do regulators, firms and their advisors deal with the risk of huge sums of money being laundered over UK crypto networks?

Since 10 January 2020, all UK cryptoasset exchange providers and custodian wallet providers have had to comply with the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs) and, from 10 January 2021, be registered with the Financial Conduct Authority (FCA) or on its list of firms with temporary registration. [3] The deadline for registration by the FCA has twice been extended, partly because of COVID-19 related delays but also due to the sheer number of firms applying and the rigorous process applied by the FCA. At the time of writing (29 June 2022), there were 35 firms with full FCA registration under the MLRs,[4] and two firms remaining under the temporary registration regime,[5] while around 90% of applications were withdrawn or refused by the FCA.[6] Around 250 unregistered cryptoasset businesses have been identified by the FCA and are liable to enforcement action.[7] The fact that so many firms, including some well-known names, withdrew their applications is a sign that many were unprepared for the high level of scrutiny applied by the FCA.

What are the UK anti-money laundering requirements for cryptoasset firms?

The MLRs, which were amended as part of the UK Government's programme to implement (and exceed the requirements of) the EU Fifth Money Laundering Directive,[8] apply to "cryptoasset exchange providers" and "custodian wallet providers",[9] with a deliberately wide definition of "cryptoasset".[10]

In summary, the MLRs require firms to:

1. Maintain an up-to-date written anti-money laundering (AML) / counter-terrorist financing (CTF) risk assessment (regulation 18).
2. Maintain and regularly update policies, controls and procedures to manage the AML/CTF risks identified in the risk assessment (regulation 19).
3. Appoint an officer responsible for compliance with the MLRs (regulation 21(1)(a)).
4. Screen all employees with roles relating to compliance (regulation 21(2)(b)).
5. Establish an independent audit function (regulation 21(1)(c)).
6. Appoint a nominated officer with responsibility for suspicious activity reporting (regulation 21(3)).
7. Maintain systems for rapidly responding to enquiries from law enforcement authorities (regulation 21(8)).
8. Ensure relevant employees receive AML/CTF training (regulation 24).
9. Apply customer due diligence (CDD) at customer onboarding and at other appropriate times on a risk-sensitive basis (regulation 27).
10. Verify customer identities (regulation 28(2)-(10)).
11. Undertake ongoing monitoring of business relationships (regulation 28(11)).
12. Apply enhanced customer due diligence (EDD) where there is a high risk of money laundering or terrorist financing, or a business relationship or transaction involves a person established in a "high-risk third country" designated by the EU,[11] or the customer is a Politically Exposed Person (PEP) or family member or close associate of a PEP, or the firm discovers that the customer has provided false or stolen identity documentation or information, or a transaction is complex and usually large, or there is an unusual pattern of transactions, and the transaction(s) have no apparent economic or legal purpose (regulation 33).
13. Take appropriate measures to identify PEPs (regulation 35).[12]
14. Retain adequate CDD and EDD records (regulation 40).

---

1 To give only one example, in March 2022 cryptoassets worth around $540 million were hacked from Ronin Network, a platform powering the mobile game Axie Infinity: www.bbc.co.uk/news/technology-60933174

2 '2022 Crypto Crime Report' (available on go.chainalysis.com).

3 Money Laundering and Terrorist Financing (Amendment) Regulations 2019/1511.

4 FCA Register: https://register.fca.org.uk/s/search?predefined=CA

5 FCA Register: https://register.fca.org.uk/servlet/servlet.FileDownload?file=0154G0000062BtF

6 UK Treasury, Written Answer UIN 6226, tabled on 24 May 2021: https://questions-statements.parliament.uk/written-questions/detail/2021-05-24/6226

7 FCA Register: https://register.fca.org.uk/s/search?predefined=U

8 Directive (EU) 2018/843

9 Defined in MLRs, regulation 14A.

10 MLRs, regulation 14A(3)(a): "'cryptoasset' means a cryptographically secured digital representation of value or contractual rights that uses a form of distributed ledger technology and can be transferred, stored or traded electronically".

11 The list of "high-risk third countries" in the Money Laundering and Terrorist Financing (Amendment) (No. 3) (High-Risk Countries) Regulations 2021 is currently: Albania, Barbados, Burkina Faso, Cambodia, Cayman Islands, DPR of Korea, Haiti, Iran, Jamaica, Jordan, Mali, Malta, Morocco, Myanmar, Nicaragua, Pakistan, Panama, Philippines, Senegal, South Sudan, Syria, Turkey, Uganda, Yemen, and Zimbabwe.

12 See the FCA's guidance (dated 6 July 2017) on identifying and risk assessing PEPs: https://www.fca.org.uk/publication/finalised-guidance/fg17-06.pdf

FCA enforcement action in relation to the MLRs has resulted in large fines, including over £264 million imposed on NatWest in December 2021 for AML/CTF breaches.[13]

What are the main money laundering risks?

Cryptoassets present various new AML/CTF risks, as criminals exploit the pseudonymous and instantaneous nature of cryptoasset transactions and their global reach to conceal funds and move them between jurisdictions, often exploiting regulatory arbitrage between countries with higher or lower levels of AML/CTF and cryptoasset compliance.

Key risks include:

1. The pseudonymous nature of cryptoassets: although the blockchain which records cryptoassets is usually public, the identities of wallet holders are not. Cryptoasset exchanges are required under the MLRs to verify the identities of their own customers, but they must also be aware of the risk of pseudonymous transactions at one remove from their customer. Particular risks are posed by users employing privacy-enhancing tools such as privacy coins or anonymity enhanced coins (AECs) (such as Monero); mixers and tumblers (which obfuscate the source of cryptoassets by pooling them from multiple wallets and then redepositing them into different wallets); CoinJoin (which performs a similar function to a mixer, but without the user having to send cryptoassets to an anonymous wallet in order to be mixed); clustering of wallet addresses; and IP anonymisers such as Tor and I2P. Criminal use of privacy coins is growing rapidly and makes up a substantial segment of all illicit activity in cryptoassets.[14]
2. Use of non-compliant or unlicensed cryptoasset exchanges, or exchanges in high-risk jurisdictions.
3. Use of money mules or fraudulent accounts opened at legitimate cryptoasset exchanges.
4. Peer-to-peer exchange platforms such as CoinSwap which allow for swapping between blockchains ("chain hopping"), bypassing regulated exchanges.
5. Cryptoasset ATMs or kiosks which may allow illicit cash to be converted into cryptocurrency or allow money launderers to cash out laundered cryptoassets.[15]
6. Stablecoins, whose value is tied to fiat currency and therefore can be used to facilitate liquidity for money laundering.
7. Use of cryptocurrency to fund terrorism, for example through unlicensed money exchanges or wallets disguised as being connected with charities.
8. Scams such as Ponzi schemes, investment scams and market manipulation scams, which together account for the largest segment (US$7.8 billion) of the c.US$14 billion in illicit cryptoasset activity in 2021.[16]
9. Ransomware attacks involving a ransom being demanded in cryptoassets (with major ransomware attacks being conducted recently from countries such as China, North Korea, and Russia). Ransomware addresses received c.US$602m in 2021.[17]
10. Darknet marketplace activity, which often also involves use of privacy coins to avoid detection when buying drugs, weapons, and other illicit material.

There are other risks including theft of cryptoassets and laundering of the proceeds; sanctions evasion; decentralised finance (DeFi) exchanges and tokens being used for money laundering or themselves becoming a target for cryptoasset thefts; chain peeling activity; and Non Fungible Tokens (NFTs) which present new risks for money laundering and market manipulation.

What anti-money laundering solutions are available?

In many ways, cryptoasset money laundering typologies follow the same patterns as money laundering through the conventional banking system: "placement" of dirty funds surreptitiously into the system, "layering" the funds by mixing them with clean or other dirty funds or transferring them to other people or other accounts (particularly across jurisdictional borders) in order to conceal their source, and then "integrating" the funds back into the legitimate economy to be used.

Therefore, in many ways the systems and controls required by cryptoasset firms to mitigate the risks of money laundering are the same as for other financial institutions. The three lines of defence model for compliance remains crucial for cryptoasset firms:

1. The first line of defence (the business itself) should take ownership of compliance risk, led by a strong "tone from the top" from senior management with robust reporting lines, rather than staff simply relying on the firm's compliance department to pick up on AML/CTF risks.
2. The second line of defence (the compliance function) must be adequately resourced and have sufficient independence, authority and access to management and the board to ensure it can operate as an effective check on the business.
3. The third line of defence (the audit function) must be independent from both the business and the compliance department and take a holistic approach to designing and applying compliance audit procedures. Most firms will need to build capacity to run their internal audit functions in-house rather than relying solely on external consultants.

Cryptoasset firms require all of the conventional systems and controls of any financial institution: a robust AML/CTF risk assessment; policies and procedures which are regularly updated based on the risk assessment; rigorous due diligence both at customer onboarding and on an ongoing basis; sanctions and adverse media screening; transaction monitoring tools; suspicious activity reporting and liaison with law enforcement authorities; a high level of AML/CTF staff training tailored to the risks posed to the business and the roles and responsibilities of different staff; internal and external assurance and audit procedures; and continuous compliance reporting to the compliance department, senior management and directors, which in turn should feed back into the assessment of risk.

---

13 See sentencing remarks of Mrs Justice Cockerill: https://www.judiciary.uk/wp-content/uploads/2021/12/FCA-v-Natwest-Sentencing-remarks-131221.pdf

14 Elliptic, 'Top 5 Emerging Trends White Paper'. See also Europol's Internet Organised Crime Threat Assessment 2021: https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf

15 The subject of the first Upper Tribunal decision on a cryptoasset exchange: Gidiplus Limited v FCA [2022] UKUT 00043 (TCC).

16 Chainalysis 2022 Crypto Crime Report 2022, p.5.

17 Chainalysis 2022 Crypto Crime Report 2022, p.38.

However, the traditional tools of AML/CTF compliance need to be adapted to the risks posed by cryptoasset businesses and emerging typologies for laundering cryptoassets.

Helpfully, some solutions lie within the problem itself. The blockchain technology underlying cryptoassets provides significant compliance advantages. Most obviously, the fact that there is a permanent ledger record of all cryptoasset transactions, which is (mostly) irreversible and (generally) publicly accessible, means that in theory every step in the chain of a cryptoasset laundering process can be traced – in a way that cannot always be done for, say, laundering through the cash economy.

Powerful compliance technologies are already in use and are being further developed to capitalise on this feature of cryptoasset transactions, including blockchain monitoring tools such as Chainalysis, Elliptic, and others. Various providers have also developed solutions for monitoring patterns in transactional activity, which can be customised according to the firm's business model and risk parameters.

However, both blockchain monitoring and transaction monitoring tools are only as good as the calibrations that are set for them and the people who operate them, so a high level of expertise and training is required to get the best out of them.

What about the future?

Money launderers, terrorist financers and fraudsters will continue to look for new ways to clean dirty funds, and regulators and firms will need to evolve with them.

Important future developments will include implementation of the "travel rule" in UK law in accordance with FATF's Recommendation 16, now due for 1 September 2023 following HM Treasury's June 2022 consultation response on amendments to the MLRs. This will require regulated businesses to obtain personal information on both the originator and beneficiary of any cryptoasset transfer above €1,000. The travel rule has already been implemented for cryptoassets by the USA, Canada, Germany, Singapore, South Korea, Switzerland, Japan, and others, so the UK will be brought in line with its peer group.

Also important will be the increased risk of sanctions evasion as a result of the wide-ranging sanctions imposed on Russia and Belarus. This is likely to manifest in several ways. Individual citizens of those countries looking to move funds via cryptoassets, because they cannot access the conventional Western banking system, are particularly vulnerable to hacking and scams. Sanctioned persons and others looking to evade sanctions will drive an increase in the laundering of assets subject to sanctions, some of which is likely to be routed through wallets controlled by organised criminals and dark networks. At the same time, illicit activity that was previously routed through the conventional banking system will be displaced onto crypto networks.

It is also likely that we will see increasing use of sanctions targeted at cryptoasset businesses themselves for facilitating sanctions evasion, fraud, and money laundering (see the US OFAC sanctions imposed to date on Suex, Chatex, Hydra and Blender).

Finally, the power of blockchain monitoring tools such as Chainalysis and Elliptic is such that firms may be able to detect evidence of criminality at several removes from their customers. So long as that evidence does not implicate their customer or create an unacceptable risk of money laundering via the firm, it is unlikely that the firm will come under a duty to report it as suspicious activity. However, depending on the nature of the evidence and the criminality indicated, it may be appropriate for the firm to file an informational suspicious activity report in order to assist law enforcement agencies. It remains to be seen whether the National Crime Agency, FCA, and other bodies internationally will provide guidance on where the line is to be drawn in this regard.

As compliance standards improve across the regulated UK cryptoasset industry, regulated firms should experience a levelling of the playing field as non-compliant firms are forced out of the market. However, wide disparities remain in regulation of cryptoasset businesses across the globe and will continue while FATF's recommendations remain to be implemented in full by most countries (including the UK, until the travel rule is implemented in September 2023).

Harbottle & Lewis

Award winning providers of Private Client advice and services.

The LEGAL 500 UNITED KINGDOM LEADING FIRM 2022

TOP RANKED Chambers High Net Worth 2022 Harbottle & Lewis LLP

harbottle.com

CRYPTO IN DISPUTE: A PRIVATE INVESTOR'S SURVIVAL GUIDE

Authored by:
Lizzie Williams
Senior Associate and Solicitor Advocate in the Dispute Resolution Group
Harbottle & Lewis

The crypto market, with its potential for rapid growth, is an enticing prospect for forward-thinking private investors but it is not without risk. What pre-emptive moves can a private investor make to reduce the chances that they end up in a crypto-related dispute?

The list below is not exhaustive, but it does highlight the variety of issues which must be considered to mitigate the risk of contentious issues for private investors investing in crypto. Seeking legal and financial advice before investing, rather than after things go wrong, is strongly recommended.

(1) Assess the regulatory position

It is paramount that an investor understands whether their investment is regulated by the Financial Conduct Authority (FCA) and protected by the Financial Services Compensation Scheme (FSCS). The FSCS protects investors' funds where they have invested with companies authorised by the FCA, up to a value of £85,000 per person. Exchange tokens, such as Bitcoin, are currently outside the scope of the FSCS, whereas security tokens (often shares in the company issuing the token) may be covered by it depending on the features of the token. If you invest in exchange tokens, you are not protected if a platform that holds or exchanges them goes out of business. That must be factored into the investment strategy.

(2) Implement security measures

A common fear amongst investors in crypto – and something that has given rise to a number of cases in which litigants have sought to freeze the assets in question - is misappropriation of cryptoassets by hackers. There are practical steps which can be taken in order to mitigate this risk.

As a starting point, a private investor should consider the type of crypto wallet in which to store their investment. With a "non-custodial" wallet, an investor is in control of and responsible for their private keys. If the key is lost, the investment is lost, so an investor should put back-up measures in place. Those measures might take the form of offline "hardware", physical wallets that store the private keys offline.

Alternatively, "custodial" wallets are available, where a third party is in control of an investor's private keys; the exchange owns the private keys and holds the cryptocurrency in their wallet, effectively on behalf of the investor. With this approach, the investor does not have the responsibility of control of their private keys, but they are relying on the security of the exchange to protect against hackers.

Another layer of protection is insurance; there are cryptocurrency wallet insurance solutions available to protect against losses arising from the misappropriation of cryptocurrency in online wallets.

(3) Read the T&Cs carefully

As dull as it might be to review the T&Cs of a currency exchange platform or other company with which the investor is contracting, they are essential reading for an investor and their legal advisors.

Those T&Cs will have an impact on the legal remedies available (if any) in the event that the investor suffers losses due to, for example, technical issues with accessing the platform or delayed transactions. They will likely determine the jurisdiction in which claims against the platform can be brought and the law governing the relationship between the investor and the platform. Whilst a private investor is unlikely to be in a position to negotiate the T&Cs, they are a factor affecting the risk profile of the investment.

(4) Additional considerations with NFTs

NFTs – or "non-fungible tokens" – are often marketed as a way to own a unique digital asset as opposed to a fungible asset such as Bitcoin. From an investment perspective, purchasing a unique asset which may go up in value is appealing. There are, however, a lot of misconceptions about what is actually being transferred by an NFT. Is it ownership or something else? Is copyright transferred?

The NFT itself is a smart contract i.e., a set of code and the token generally links to a digital asset. It will depend on the circumstances and the seller's T&Cs, but often what is being transferred to the investor is a licence to use the digital asset for their personal purposes; they will generally not acquire any form of copyright. It is essential that any investor in NFTs understands what they are purchasing.

From a valuation perspective, it will be important to carry out due diligence on the seller and verify the chain of title of the NFT and the asset to ensure their provenance. If an investor is misled as to what they are buying, they may face difficulties in obtaining legal redress, particularly if the contractual counterparty cannot be readily identified, so an investor should assume they are buying the NFT "as is".

The issue of identifying the contractual counterparty is not unique to NFTs. With any crypto investment, a private investor will be better placed to resolve any dispute if they know exactly which entity or person they are contracting with, their contact details, where they are based, and their financial standing. Legal advice should be sought on the prospects of obtaining redress against them if things go wrong.

(5) Unusual or complex investments

There are myriad crypto-related investments available, all with their own unique considerations.

In certain circumstances, it will be advisable for an investor to enter into natural language agreements with their contractual counterparty which co-exist alongside and complement the blockchain transaction. These will be drafted by lawyers and will clarify rights and obligations including, for example, warranties in relation to the nature of the investment and allocating liability for code malfunctions.

Similarly, sometimes it will be advisable for an investor to seek that the code for a particular transaction is verified by a

professional firm specialising in checking the terms of smart contracts to ensure that the code does not contain bugs or errors, is not vulnerable to hacking or exploitation, and will perform exactly as anticipated by the investor.

Hopefully, we are working towards a world where coders and lawyers frequently collaborate in the creation of smart contracts where parties can benefit from the performance certainty of self-executing code on the blockchain, alongside the protection of a properly drafted natural language agreement. That is likely to be considered the gold standard and an approach worth considering for any high value investment.

(6) Consider the tax implications

The taxation of cryptocurrency is a complex area and advice should be sought in advance on the tax implications of any crypto investment.

In general, where crypto is treated as a store of value, buying and selling it will fall within the Capital Gains Tax rules, and where the indicators of trading are prevalent, income tax rules apply.

In the context of DeFi (decentralised finance), interesting questions arise around whether an investor's returns on a crypto investment constitute interest for the purposes of taxation. On the basis of the current case law on the definition of interest, and the fact that cryptocurrency is not given the same treatment as fiat currency, it appears the return may amount to a revenue receipt rather than interest and taxed accordingly.

Before investing, an investor would also be well advised to determine in advance how they will lawfully transfer the rewards of their investments into the non-crypto, traditional economy. The impact of money laundering regulations should be taken into account, as should the policies of individual banks, as some are considered more crypto-friendly than others.

(7) Investments through trusts

Clearly, where trustees are making investments for the benefit of trust beneficiaries, there is a further layer of considerations to be thought through and advice to be obtained to ensure that the trustees and their investments are appropriately protected and that the trustees' fiduciary duties are adhered to.

(8) Doing the homework

There is no substitute for swotting up on what you are investing in.

If an investor fully understands the applicable contractual provisions, the meaning of the code, the legal nature of what they are investing in, the tax implications of the investment, the reputation of the seller, the volatility of the market, the provenance of the asset, the relevant blockchain transactions, and their available legal recourse if things go wrong before making the investment, an investor will be better placed to assess the value of the investment, less likely to encounter an unexpected dispute, and more able to deal with any contentious issues swiftly and effectively, should they arise.

Wilberforce
CHAMBERS

wilberforce.co.uk

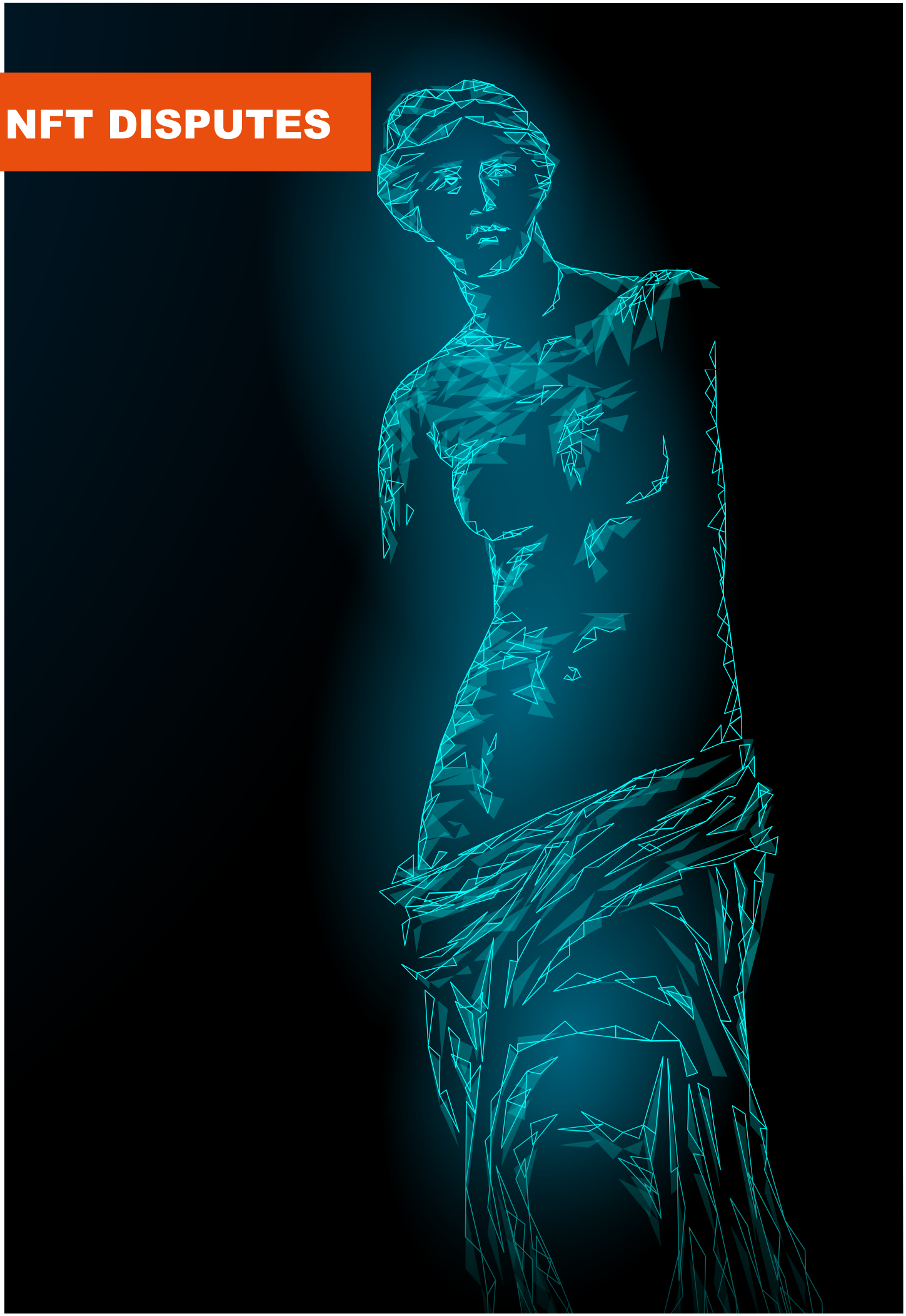
We are one of the leading commercial chancery sets of chambers in the UK, where barristers are involved in some of the most intellectually challenging and legally significant matters undertaken by the Bar today. Our specialists have been involved in many of the most high-profile fraud, insolvency and asset recovery cases of recent times, both in the UK and across numerous international jurisdictions, and we also offer a range of advisory services to our clients.

> **"Wilberforce is the best chancery commercial chambers there is."**
>
> The Legal 500, 2022

A top-ranked set in The Legal 500 and Chambers & Partners, and winner of Insolvency & Restructuring Chambers of the Year at the 2021 TRI Awards.

+44 (0)20 7306 0102 chambers@wilberforce.co.uk
Wilberforce Chambers, 8 New Square, Lincoln's Inn, London, WC2A 2QP

NFT DISPUTES



Authored by:
Gilead Cooper QC
Barrister
Wilberforce Chambers

The first known NFT, "Quantum", dates from as long ago as May 2014. It was created or "minted" by the artist Kevin McCoy and in June 2021 it was sold through Sotheby's for US$1.47 million. Within a year, the sale had given rise to litigation: Free Holdings Inc. v McCoy et al., (NYSD-1:2022-cv-00881). This is not the only case involving NFTs to have already emerged: within the last couple of years, there have been several such cases, mostly in the US. Examples include Miramax LLC v Tarantino (C.D. Cal. 2021), in which the studio is suing the director over an NFT relating to the movie Pulp Fiction; then there is Hermès Int'l et al. v Rothschild, Index No. 1:22-cv-384 (S.D.N.Y), in which there is a dispute over imaginary Birkin bags; and TamarindArt, LLC v Husain et al, Index No. 1:22-cv-0595-AT (S.D.N.Y), where there was an issue as to whether NFTs based on a 60-foot-long mural by the artist Maqbool Fida Husain would violate the copyright vested in the estate of the artist. The list goes on. Now a case involving NFTs has reached the English court in which the court has granted a freezing order: Osbourne v Persons Unknown & Ozone Networks Inc., although at the time of writing, the reasoned judgment has not yet been handed down. And in another as-yet-unreported decision, the Singapore High Court has very recently granted an injunction freezing the sale of a Bored Ape Yacht Club NFT.

The advent of cryptoassets has given rise to a number of novel questions of law. NFTs are a specific kind of cryptoasset and share many of the characteristics of cryptocurrencies (of which Bitcoin and Ether are the best known), including, importantly, a basis in blockchain technology. They also exhibit a number of unique features of their own.

For lawyers, the first and fundamental question relating to all types of cryptoassets is whether as a matter of property law they are recognised as a species of property at all. So far, the courts that have had to consider this question have unanimously answered "yes". But with the exception of a couple of cases from Singapore and New Zealand, these decisions have all been interlocutory: these decisions merely mean that there is a sufficiently arguable case to justify some sort of interlocutory relief such as a freezing injunction or Bankers Trust order. Many of these decisions have adopted the reasoning of the UK Jurisdiction Taskforce in its Legal Statement on Cryptoassets and Smart Contracts, which considered the case law and concluded that cryptoassets were indeed a species of intangible property. In the recent Osbourne case mentioned above, an injunction was granted in respect of stolen NFTs on the basis that they, too, could be "property" for the purposes of English law.

Conceptual problems remain

It is tempting, therefore, to regard the question as settled, at least so far as the common law is concerned. But some conceptual problems remain. What, precisely, is the "property" that is recognised? Here, a distinction may be drawn between cryptocurrencies like Bitcoin and NFTs. A unit of cryptocurrency exists only in computer code; an NFT, on the other hand, is a piece of digital code associated with an "asset" that is not itself held on the blockchain - the cases mentioned above provide some examples. Often, the "asset" is a digital artwork of some kind, or a digitised version of a physical artwork which is stored elsewhere. In the case of the artwork "Everydays: The First 5000 Days" by the digital artist known as "Beeple", a compressed file in JPEG format, with which the NFT is associated, is held on a decentralised file sharing service that is part of the Internet. It can be downloaded from there by anyone. The original uncompressed version is (presumably) still held somewhere on a computer owned by Beeple himself.

The process by which an NFT is "minted" from the original asset is not a standardised process, but for the purposes of legal analysis it is important to remember that it is not the asset itself that is acquired by the purchaser. Although NFTs are sometimes described as "certificates of ownership", suggesting that the owner of the NFT somehow owns the off-chain asset, that expression should be understood in a metaphorical rather than a literal sense. The owner of the NFT does not own the physical medium – such as the computer hard drive or memory stick – on which the original is stored. Furthermore, the creator retains (at least in the majority of cases) the copyright.

What does the purchaser actually own?

What, then, does the purchaser of an NFT acquire? It is not easy to give a fully satisfactory answer: the purchaser does not own the original, nor does he own the right to make copies. As for the information encoded in the version of the artwork with which the NFT is associated, that is incapable of being the subject-matter of ownership, at least under the common law, which pure information is not recognised as property. He does not even own the "token" which resides on the blockchain. What, then, is left? According to one analysis, the purchaser of an NFT acquires no more than the ability to transfer an identifiable piece of code on the blockchain to another person.[1] That is to say, he knows the private key (a string of numbers) which enables him to pass the control of the token to another private key.

It is difficult to justify characterising that ability as a legal right under the law as it currently stands. There is no-one against whom it is enforceable in a court of law. It is "enforceable" only in the sense that (and to the extent that) it will be executed by a "smart contract" (which is not a legal contract at all). Could it be stolen? In theory, an "owner" could simply memorise his private key but in practice, the key will be recorded in some way, usually by being stored on a computer or in a "hard wallet". The computer or hard wallet could certainly be stolen but if a hacker merely gains access to the key (which is pure information) and then uses it to transfer the NFT to himself, what can he be said to have "stolen"? All he has actually done is to substitute his own private key for that of the previous one on the blockchain.

1 R. Graham (20 March 2021), "Deconstructing that $69million NFT", Errata Security at https://blog.erratasec.com/2021/03/deconstructing-that-69million-nft.html#.YGKbj68zaUk

In one case, Dixon v R [2015] NZSC 147, the New Zealand Supreme Court held that a video file that had been copied from a security camera and then sold to the press constituted "property" for the purposes of the New Zealand Crimes Act 1961. The video showed a member of the British Royal Family "socialising intimately" with a female at a bar and the accused had tried to sell a copy to the press. The court held that the digital files were "property" for the purposes of the relevant statute but for reasons that are highly debatable. The decision has been persuasively criticised: see Bridge, Gullifer, Low & McMeel on The Law of Personal Property (3rd edition), Chapter 8.

It is often said that NFTs confer no more than "bragging rights". This view may suggest that the purchasers of such rights are gullible suckers who have been duped into throwing their money away on something worthless: there was much schadenfreude when the purchaser who had paid US$2.9 million for an NFT of Jack Dorsey's first tweet tried to sell it (with an asking price of US$48 million) and received an offer of only a few hundred dollars (or possibly thousand – the reports vary). On the other hand, it should not be forgotten that many "collectible" assets are valued for sentimental reasons that are difficult to justify on objective grounds: think of postage stamps, first editions, movie or sporting memorabilia, autographs. These have little or no intrinsic value but are prized and valued on the basis of scarcity or snob appeal (compare the Veblen effect, according to which the demand for certain types of luxury goods increases as the price goes up – in apparent defiance of the usual law of supply and demand).

There is no doubt that NFTs represent economic value, although it is debatable whether they will continue to trade at the astonishing sums that have been reported in the press in the last few years. The market currently resembles a gold rush. But the technology is unlikely to go away and the security issues that have plagued it (despite its theoretical invulnerability) may well be improved. The safest prediction is that the courts are unlikely to be idle; all computer software contains bugs, and ingenious hackers will continue to look for ways to exploit them. Furthermore, there will always be scope for ordinary human error. These ingredients provide a reliable recipe for litigation for years to come.

maitland CHAMBERS

Maitland Chambers is one of the leading sets of barristers' chambers in the UK. Based in London's Lincoln's Inn, we offer legal advice and advocacy of the highest quality both domestically and internationally.

With a vast number of specialists in fraud, asset recovery, insolvency and restructuring, our members act for a diverse client base and regularly appear in courts and tribunals of every level in England and Wales (including the Supreme Court and the Privy Council) and internationally, particularly in the BVI, the Cayman Islands, Bermuda, Dubai, Singapore, Hong Kong, Gibraltar and the Channel Islands.

"An impressively deep stable of elite silks and juniors"

Chambers UK

CONTACT

For further information, please contact our Clerks using the details below:

John Wiggs - Senior Clerk
jwiggs@maitlandchambers.com
+44 (0)20 7406 1251

Robert Penson - Deputy Senior Clerk
rpenson@maitlandchambers.com
+44 (0)20 7406 1258

Luke Irons - Deputy Senior Clerk
lirons@maitlandchambers.com
+44 (0)20 7406 1257

7 Stone Buildings
Lincoln's Inn
London
WC2A 3SZ

www.maitlandchambers.com

LAW UNDER ATTACK – LEGAL REMEDIES AGAINST PERSONS UNKNOWN TO COMBAT CYBER ATTACKS

Authored by:
Darragh Connell
Barrister
Maitland Chambers

Over the past year, law firms, barristers' chambers and legal professional bodies have increasingly emerged as principal targets for malicious and sophisticated cyber attacks designed to unlawfully extract ransom payments from legal professionals.

By way of indicative example of the widespread nature of such attacks, on 26 April 2022, the IT systems of both the General Council of the Bar of England and Wales and the Bar Standards Board were taken offline as a consequence of a cyber attack in an effort to "restore all systems and services and extend security arrangements".

Notably, there have been a number of recent cases where legal services firms have successfully obtained injunctive relief from the English courts against persons unknown responsible for these types of attacks.

Whilst there are myriad regulatory and reputational issues created by cyber attacks, this article seeks to provide an overview of the applicable legal principles by which injunctions can be obtained against persons unknown responsible for such attacks; common issues that arise in the context of injunction applications against persons unknown; and recent injunctions obtained against those responsible for cyber attacks against legal services firms and organisations.

1. Applicable Legal Principles in respect of the 'Persons Unknown' Jurisdiction

The right to obtain an injunction against an unknown person was first established in Bloomsbury Publishing Group v News Group Newspapers Ltd [2003] EWHC 1087 (Ch) which concerned the theft from printers of the unreleased fifth Harry Potter book which was being offered to newspapers by unknown individuals prior to its official publication. In granting the relief sought, the High Court recognised that the court had jurisdiction to make orders against such persons unknown provided that:

"…the description used must be sufficiently certain as to identify both those who are included and those who are not. If that test is satisfied then it does not seem to me to matter that the description may apply to no one or to more than one person or that there is no further element of subsequent identification whether by way of service or otherwise".

In the subsequent notable case of CMOC v Persons Unknown [2017] EWHC 3599 (Comm), HHJ Waksman QC extended the jurisdiction to make orders against person unknown to freezing injunctions. The case itself involved a significant fraud by persons unknown infiltrating the email account of one of the claimant company's senior management in order to send fictitious payment instructions, purportedly from the said manager. As a result, a number of very large payments were sent out from the company's bank account held with Bank of China in London to various other banks around the world.

In a valuable judgment for fraud litigators, the court in CMOC provided a principled basis for the extension of the jurisdiction against persons unknown in fraud cases noting as follows:

"there is a strong reason for extending the principle [relief against persons unknown] which is that the freezing injunction can often be a springboard for the grant of ancillary relief in respect of third parties, which arguably could not get off the ground unless there has been a primary freezing injunction. That is very much the case in fraud litigation…".

More recently, in AA v Persons Unknown [2019] EWHC 3556 (Comm), Bryan J. granted an interim proprietary injunction against persons unknown responsible for a cyber attack on a Canadian insurer where a ransom had been paid. The injunction was also obtained against other persons unknown who controlled a wallet with a cryptocurrency exchange where a substantial proportion of the relevant ransom payment had been paid.

2. Common issues when obtaining injunctive relief against persons unknown

Hearing in Private

A frequent issue that arises in the context of any application against persons unknown is a desire on the part of the applicant for the hearing of the initial application to take place in private so as to avoid 'tipping off' the relevant unknown wrongdoer.

Conducting a hearing in private ostensibly conflicts with the constitutional principle of open justice which is a fundamental aspect of the law of England and Wales. CPR r. 39.3(3) sets out the relevant exceptions to the open justice principle. Insofar as relevant for the purposes of this article, it provides as follows:

39.2(3) A hearing, or any part of it, must be held in private if, and only to the extent that, the court is satisfied of one or more of the matters set out in sub-paragraphs (a) to (g) and that it is necessary to sit in private to secure the proper administration of justice –

(a) publicity would defeat the object of the hearing;

…

(c) it involves confidential information (including information relating to personal financial matters) and publicity would damage that confidentiality;

…

(e) it is a hearing of an application made without notice and it would be unjust to any respondent for there to be a public hearing;

…

(g) the court for any other reason considers this to be necessary to secure the proper administration of justice.

Most notably, CPR r.39.2(3) is mandatory in its terms. In other words, if the court is satisfied that one or more of the grounds identified in (a) to (g) apply, then the court must hold the hearing in private.

In cases concerning cyber attacks which involve blackmail and extortion, it is now more common for the court to permit hearings to be held in private. This is because the interests of freedom of expression are naturally tempered by the criminal conduct in question and where injunctive relief is sought to thwart blackmailers.

Service

A second common issue that arises when an applicant seeks relief against persons unknown is the knotty question of service. One difficulty, of course, arises in relation to unknown defendants, which is that because they are persons unknown it is not as yet known what jurisdiction they are in. They could be domiciled in any jurisdiction. This is not an unusual problem and the courts have developed a pragmatic approach to grapple with this issue.

In Clarkson plc v Persons Unknown [2018] EWHC 417 QB, the applicant company brought proceedings for an injunction to prevent unknown persons from disclosing or using confidential information illegally obtained from the company's IT systems in circumstances where the unknown defendants threatened to publicise the information unless a very substantial sum was paid. The court granted the applicant company an interim injunction prohibiting the persons unknown from communicating or disclosing certain information to any third party or using it in any other way and made an order permitting the applicant to serve the claim form on the e-mail address used by the defendants to make the relevant blackmail threats.

In 4 New Square v Persons Unknown (unrep. 28 June 2021) - which involved a cyber attack on a barristers' chambers - Steyn J. was prepared to make an Order that the claimant barristers were not required to serve confidential witness evidence on the persons unknown unless and until the defendants identifies themselves and provided an address for service. This was deemed appropriate because sending the evidence relied upon to the defendant could lead to its further misuse.

In subsequently entering default judgment in the 4 New Square v Persons Unknown case, Nicklin J. also made a final Order precluding non-parties from being provided with copies of the confidential witness statements or confidential schedules or exhibits to the applications and to the skeleton arguments without further court order in order to protect the relevant confidential information in respect of which the claimant barristers sought to restrain publication.

3. Recent injunctions obtained against those responsible for cyber attacks on legal professionals.

There have been numerous recent injunction applications brought by law firms seeking to restrain disclosure of confidential client information following cyber attacks. Two cases are worthy of specific mention, namely The Ince Group Plc v Persons Unknown [2022] EWHC 808 (QB) and Ward Hadaway LLP v Persons Unknown [2022] 4 WLUK 217.

The Ince Group Plc v Persons Unknown [2022] EWHC 808 (QB):

On 1 April 2022, Mr Justice Saini granted urgent interim prohibitory and mandatory injunctions in favour of the claimant law firm which had been subject to a cyber-attack on or around 13 March 2022, during which persons unknown had obtained certain confidential data belonging to the firm. The so-called threat actors threatened to publish the stolen data on the dark web if the law firm did not pay a substantial ransom.

The court was readily prepared to grant the prohibitory injunction where the basic elements of a classic breach of confidence claim had been established by the claimant. In particular, the claimant had title to sue, there was clearly a duty of confidence owed by the defendant, and the underlying material was clearly confidential. Given the threatened public disclosure, the court could see no basis for any public interest in the publication of the material. Inevitably in such a case, the court concluded that damages would not be an adequate remedy.

The judgment is notable since the court was also prepared to grant an interim mandatory injunction requiring the unknown defendants responsible for the cyber attack to deliver and/or delete and/or destroy the information they had stolen.

Ward Hadaway LLP v Persons Unknown [2022] 4 WLUK 217.

The claimant law firm continued an interim injunction against persons unknown following a cyber attack on its IT systems. The persons unknown had uploaded a number of files to a public website. It appeared likely that those files were encrypted, so while they could be downloaded by anyone, they were not readable without a decryption key which the unknown defendants would be willing to provide for payment; or, in accordance with their threat, they might upload the files in a decrypted form.

The court had no hesitation in granting both prohibitory and mandatory injunctions save that Edwin Johnson J. made clear that the injunction should not continue indefinitely, and a long stop of 31 October 2022 was provided for in the Order.

Conclusion

The courts have repeatedly shown a willingness to assist those individuals and companies who have fallen foul of cyber attacks by granting appropriate injunctive relief against the persons unknown responsible for this criminality. Regrettably, it appears likely that yet further attacks on the legal industry will necessitate injunctive relief of this nature on a regular basis.

Insolvency and asset recovery

We are the market leading Insolvency and asset recovery practice as recognised regularly by Who's Who Legal. We are continuously developing and evolving our practice to respond to the needs of global demand for our services.

We focus on understanding the unique situation of each case and work with you to devise and implement asset recovery solutions. The cases we deal with will often have elements of fraud, regulatory breaches or international angles.

Global asset recovery using cross-border insolvency powers

We have the largest asset recovery practice in the UK and our team focuses on maximising the recoveries of assets for creditors and the victims of fraud.

We adopt innovative strategies incorporating the powers we have as insolvency practitioners and receivers. We recognise the importance of acting at short notice and have experience of handling all types of cases.

Our services

- Asset tracing and global asset recovery, including digital assets
- Contentious insolvency
- Funding enforcement of judgments and awards
- Joined up global approach across the key offshore financial centres
- Offshore investigations and insolvency
- Corporate Intelligence
- Personal insolvency
- Acting as receiver or administrator over deceased estates
- Enforcing matrimonial awards
- Taking director appointments

Visit grantthornton.co.uk to find out more, or contact one of our Insolvency and asset recovery partners:

Kevin Hellard
Practice Leader
T +44 (0)20 7865 2478
E kevin.hellard@uk.gt.com

Sean Croston
Partner
T +44 (0)20 7728 3172
E sean.croston@uk.gt.com

Hannah Davie
Partner
Estates and Family Disputes
T +44 (0)20 7865 2849
E hannah.davie@uk.gt.com

Colin Diss
Partner
T +44 (0)20 7865 2511
E colin.diss@uk.gt.com

David Ingram
Partner
T +44 (0)20 7865 2367
E david.ingram@uk.gt.com

Amaechi Nsofor
Partner
T +44 (0)20 7865 2388
E amaechi.nsofor@uk.gt.com

Nick Wood
Partner
T +44 (0)20 7728 2426
E nick.s.wood@uk.gt.com

David Bennet
Partner
T +1 284 346 9975
E david.bennett@uk.gt.com

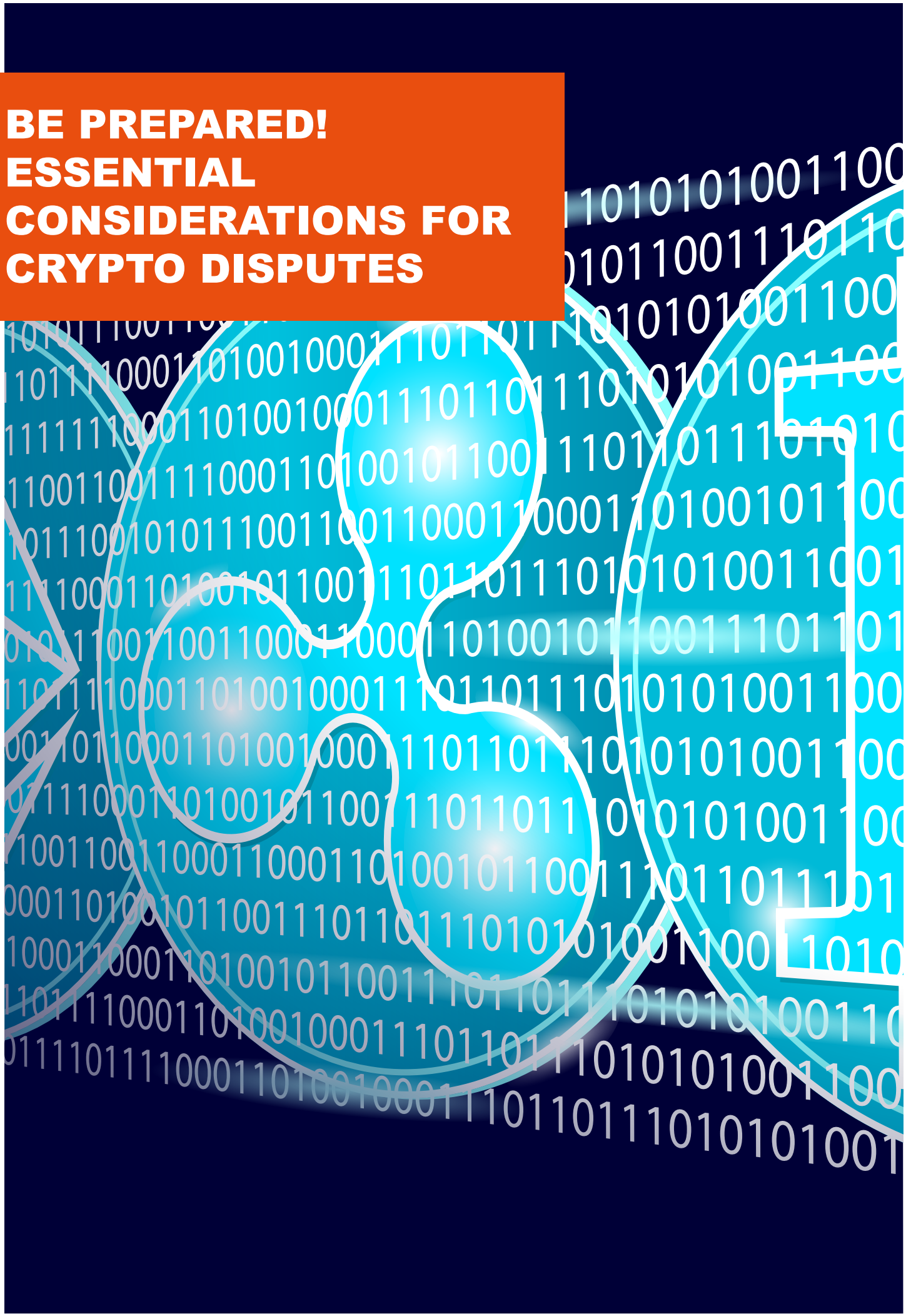
Hugh Dickson
Partner
T +1 345 769 7203
E hugh.dickson@uk.gt.com

Margot MacInnis
Partner
T +1 345 769 7203
E margot.macInnis@uk.gt.com

Grant Thornton

DS3180

BE PREPARED! ESSENTIAL CONSIDERATIONS FOR CRYPTO DISPUTES



Authored by:
Carmel King
Director, Insolvency and Asset Recovery
Grant Thornton UK

Litigation in the cryptosphere is generally regarded as nascent but rapidly developing. In just three years, for example, the English Court has confirmed that Bitcoin is capable of being property (AA c Persons Unknown & Ors); that the ***lex situs*** of cryptocurrency is where the owner is based (Ion Science Ltd v Persons Unknown & Ors); that cryptoassets are capable of being held on trust (Wang v Darby); and that cryptoassets may not be used as security for costs (Tulip Trading Ltd v Bitcoin Association for BSV). Many cases heard in the English Court will be in support of asset recovery and involve applications for freezing orders, disclosure orders, and orders to allow the recovery of cryptoassets. In such cases, it is absolutely essential to get the underlying basics right before initiating the action.

In most scenarios we have seen to date, the transactions surrounding the misappropriated assets will be visible on a public blockchain. Blockchain explorers are widely available to search the blockchains for transactions, addresses, tokens, prices and other activities. Specialists use sophisticated platforms with clustering and attribution features to provide broader context and a higher degree of confidence around the identification of addresses and wallets. These platforms are constantly evolving in an effort to keep up with the efforts of fraudsters; for example, Chainalysis has just announced a cross-chain DeFi tracing capability. This work requires training and experience to analyse results and draw informed conclusions. The results are frequently used in support of the various applications for relief previously described.

It really is imperative to use the right expert in carrying out the analysis. You might argue that of course I would say this! Fair enough; but given that an application for a freezing order carries with it a cross-undertaking in damages, don't come crying to me after you applied to freeze the wrong wallet, resulting in your client's liability for the worldwide shutdown of a multi-billion dollar exchange! Let's speak before that happens. It is also worth highlighting that victims of fraud in this space can be highly technically proficient, keen on securing the return of their funds, and not afraid to move between professional advisors. The use of sub-standard technical materials in a court application could lose you a client and cause reputational damage.

Getting the basics covered at the outset will ensure a good set-up for what could be a lengthy matter. Conducting some corporate intelligence at the outset can provide a wider context and potentially other angles of attack in addition to proceedings. Are there any companies involved in the fraud, and are they in jurisdictions where they might be placed into liquidation, with all of the investigation and litigation powers that are bestowed upon the liquidator? Can this case be linked to any other frauds, or can other victims be identified to grow the claim? Can the fraudsters or any third-party facilitators be identified, and what is their asset status? The speed of potential dissipation of cryptoassets is a challenge and from the outset, a basic consideration should be the alternative routes to recovery.

Innovation is key

In a relatively new and fast-paced area of law, innovation is key. The best litigators are thinking outside the box, trying new approaches and pushing the boundaries of what has been achieved so far. Inevitably, some approaches will be more successful than others and without hindering that innovation, it is essential to think strategies through and consider the consequences of step one of the multiple steps that will inevitably be required before a recovery is made. For example, litigators may rush to apply for a worldwide freezing order on the basis of a risk of dissipation. I have seen cases where this has been the wrong decision: a proprietary injunction would have been a better strategic move in terms of specifying particular property, obtaining disclosure orders, and ultimately third-party debt orders and return of the cryptoassets.

During our Cyber War Game at TL4's FIRE International in Vilamoura recently, Steven Gee QC very eloquently explained the issues around obtaining a Norwich Pharmacal order against a bank where funds had been transferred onwards to a crypto exchange. Orders for the freezing of wallets and the provision of information are typically obtained against exchanges in the early stages of this sort of dispute. Interactions with exchanges are changing. Where previously, litigators found it difficult, if not impossible, to enforce orders obtained in an English Court against exchanges based everywhere and nowhere, increasing regulation and a desire to become more mainstream have caused exchanges to nail their flags to certain jurisdictional masts, and groups such as CFAAR (the Crypto Fraud and Asset Recovery Network) have enabled the sharing of best practice and tools for leverage amongst practitioners.

Don't be fooled into thinking it will be easy though. We may lazily compare exchanges to banks in conversation, but exchanges come from a fundamentally different philosophy: innovation, decentralisation and anonymity versus regulatory responsibility, consumer protection and compliance armies. Or perhaps, a fairer observation is that the banks have had longer to at least give the appearance of regulatory compliance!

A January 2022 Reuters report describes Binance as withholding information from regulators, maintaining weak KYC checks on customers and acting against its own compliance department's recommendations, whilst simultaneously in public lauding its own KYC practices and publicly welcoming regulatory oversight. The withholding extended to declining to provide information to German police and lawyers representing victims of crime to the tune of several million euro suspected to have been laundered through the exchange. Binance has denied the allegations. An August 2021 report on Coinbase indicates that in that year, thousands of US customers were victims of account takeover hacks. Coinbase's response to complaints amounted to, "There is no credible or supportable evidence that the compromise of your login details was the fault of Coinbase. As a result, Coinbase is unable to reimburse you for your alleged loses".

Practitioners need to leverage everything available to them, as it may not be much. An email address? A known (or potential) jurisdiction? A CFAAR contact who has already walked that path? Leverage it. And please, please give care to the wording of orders sought. You may not be able to engage the exchange in a meaningful way. Correspondence may be more similar to dealing with the more obtuse sort of defence solicitor (apologies to the obtuse defence solicitors reading, I get that it's an approach), with the need to constantly repeat the basic facts, rebut incorrect assertions and for extended communication where more than one piece of information is required. Try to keep the order simple to avoid the hazards of one wallet being frozen where several are required to be, or disclosure being provided around one wallet where the order should apply to all wallets held by the target. This can be a real risk in situations where the target is persons unknown, and reliance for disclosure is placed completely on the exchange.

The custodianship issue

Finally, custodianship. The dispute is (almost) concluded, happily in your favour. On behalf of your client, you are now proudly in possession of 50 BTC (due to word count limitations, trust when I say there are reasons you settled in BTC). Don't leave it until the end to think about how to store and distribute – this is the whole point of the exercise and should have been considered very early on. Are you going to use hot or cold storage? Does storing on an exchange offer adequate protection for your client? Probably not. In January this year, Crypto.com admitted that 400 customers' accounts were compromised in a hack with losses of somewhere between US$15 million and US$33 million worth of ETH.

Can you ensure the security of the private key? Should you consider the services of an insured, regulated custodian? Probably. Again, exercise caution. Not all is as it seems in this space and you want the real experts rather than the aspirational kind. Traditional custodians have broadly not yet engaged with the specific requirements for the maintenance and storage of digital assets, and some new players in the market are not necessarily focused on compliance. What is the strategy if the settlement is not in BTC, but something more alternative such as OKB, DOT or Space G.O.A.T.? Seek expert advice on the sale of these assets if that is the planned course of action. The release of too many tokens in a volatile market could have catastrophic consequences, dramatically reducing or entirely destroying value for your client.

Digital assets are relatively new in litigation and like many assets, the practical aspects of dealing with this category and the infrastructure surrounding it requires forethought and engagement with specialists. That being said, it's not all negative. This nascent area of litigation is fast-paced and exciting, ever-changing, and ready for innovators to push the boundaries.

withersworldwide

Modern families are changing and the law is too

We are leading the way in adapting family law to give our clients more options

withersworldwide.com/changingfamilylaw

SHOW ME THE MONEY – DIGITAL ASSETS IN DIVORCE

Authored by:
Katharine Landells
Family Law Partner
Withers

Crypto assets are here to stay. Understand it or not, trust it or not, digital wealth is a feature of our current landscape and will certainly be a main feature in the years to come and ignorance is not going to be bliss for advisors in the private wealth sector.

Back in the early 2000s, I spent hours trying to explain to my grandmother how to send an email on her new computer. I had to leave her detailed instructions on a spiral bound notepad which she kept next to her 'machine'. They helped as a general rubric, but my grandmother never really understood how it all worked. It was a total mystery to her and so when things went wrong, or she called up a menu that she did not understand, or the computer crashed, she just phoned me - which, in the days of dial up internet, complicated matters even further.

For advisors in the private wealth space, the time has come where those who do not really understand how crypto assets work are going to find themselves at a real disadvantage, not just when it comes to their relationships with their clients, but more importantly, when it comes to presenting, evaluating, and securing digital assets for those they act for. But the good thing is that most of us now have a level of digital knowledge that my grandmother could never aspire to, so advancing that knowledge is not going to be as challenging. Notes in biro in a notebook might still help.

In many families, couples do not share the granular detail of their financial positions, even if they have shared a broad synopsis. And typically, one spouse will have a detailed understanding and control of the financial assets with the other being in relative ignorance. Those assets could be cash holdings, equities or carried interest earned through employment, shares in a founder-led or family business, private equity investments, or digital assets. In terms of the dynamic, that often results in there being one spouse who is an information holder, and one spouse who is working to get up to speed.

That catch- up game in the family law world involves disclosure, questions, and evidence gathering. And it requires the lawyers on board to ask the right questions, analyse the answers, and carefully consider the presentation given of the information. It also brings into play whatever dynamic existed during the course of the marriage. Any lack of trust will almost always then be played out in the financial disclosure exercise.

When it comes to digital assets, and particularly cryptocurrency, there are some very significant advantages to be gained simply because of the way the blockchain works. By way of explanation for those who are still in the spiral bound notebook phase, anyone who holds cryptocurrency will do so through a wallet and transactions in cryptocurrency in the wallet will be evidenced on the blockchain. The blockchain transactions are publicly available using transaction explorers. And so you can put a wallet address into a blockchain explorer and all of the transactions on that wallet and the balance of it will be visible.

Big patterns in small details

The information revealed can be incredibly useful but, unlike a bank statement, where you can see to whom or from whom debits and credits were made, crypto transactions are given long hash addresses. And so it is never possible to see more than patterns of transactions. It is a bit like going to the corner shop and getting a basic printout of the till receipt. You can see all the transactions that go through the till, but you do not know who was buying or what they were buying. What you could see would be patterns – so for example you could see many transactions for £1.29 and if you know that a litre of milk is £1.29 then you could assume that all of those transactions are for milk. Looking at transactions in a wallet held by one spouse can reveal patterns that can be investigated – regular payments to another wallet address, large payments to a wallet address not disclosed, or receipts in from a source not otherwise identified.

For those in the position of seeking information in relation to digital assets, the public nature of the blockchain is the saving grace in a world that is otherwise completely anonymous. For those in the position of having to provide information, the onus is going to be even greater in that context to show that the information given has been complete and transparent, giving proper details of the transactions made, with public key information that enables an audit of that information to be undertaken in the same way that detailed bank statements are given. There are many companies now in the market who will also provide forensic analysis services, and where there is doubt as to the veracity of disclosure given, a jointly appointed expert to report on the extent of digital holdings is going to be important to resolving outstanding issues.

Reassuringly for some clients, hiding assets or obstructing their recovery is no longer as easy as it was when it comes to digital assets. Case law is now being made in relation to the freezing of NFTs and crypto currency, and the exchanges are more and more willing to secure crypto currency accounts where there is a dispute, not least so that their own reputations are not tainted as being associated with criminal or fraudulent activity. And with the volatility of the digital assets market seemingly here to stay, there is also a real investment risk associated with the idea that a spouse might put all their assets into crypto, just to defeat financial claims on a divorce. But the biggest reassurance for any advisor will come through knowledge and understanding in detail how this world works.

ThoughtLeaders
navigate the legal maze

Meet ThoughtLeaders

Paul Barford

Founder / Director
020 7101 4155
paul@
thoughtleaders4.com

Chris Leese

Founder / Director
020 7101 4151
chris@
thoughtleaders4.com

Danushka De Alwis

Founder / Director
020 7101 4191
danushka@
thoughtleaders4.com

Maddi Briggs

Strategic Partnership Manager
07825 557739
maddi@
thoughtleaders4.com

Yelda Ismail

Marketing Manager
yelda@
thoughtleaders4.com

Georgina Hatch

Consulting Editor
georgina@
thoughtleaders4.com