Episode 8 –The Case of The Missing Crypto with Chris Whitehouse

Alice Hello, and welcome to Taxing Matters, your one stop audio shop for all things tax brought to you by RPC. My name is Alice Kemp and I will be your guide as we explore the sometimes hostile and ever-changing landscape that is the world of tax law and tax disputes. Taxing Matters brings you a fortnightly roadmap to guide you and your business through this labyrinth. In case any of you miss any crucial information or just want some bedtime reading, there is a full transcript of this and indeed every episode of Taxing Matters on our website at www.rpc.co.uk/taxingmatters.

Alice In the recent past with all of the hype around crypto, Taxing Matters has looked at a couple of different aspects of the emerging crypto asset world including the launch of CFA, the Crypto Fraud and Asset Recovery Network, which will be linked in the show notes and also the rise of criminal proceedings in relation to crypto fraud but today we thought we might do something different.

It is not an exaggeration to say that there has been a huge increase in crypto fraud, with many financial institutions poised to deal with a wave of scams but if you are caught up in a crypto fraud or crypto scam what should you do and how does the law help.

Joining me today to discuss the steps you can take is Chris Whitehouse. Chris is a senior associate here at RPC who is one of the major drivers between the CFA network and a member, like me, of RPC crypto asset practice group. Chris has a science background and a more than theoretical understanding of the blockchain plus a passion for all things crypto. So Chris, welcome back to Taxing Matters.

Chris Thanks Alice, delighted to be back.

Alice Let's launch right into it. There has been a crypto fraud, we've talked about this before, what are we doing next?

Chris The critical thing is to act quickly. If you discover that you have been a victim of a crypto fraud, be it a confidence trick, somebody swiped your password, or anything like that, you really want to get lawyers and a blockchain tracing company on board as soon as possible. Now there are two reasons for this, the first is a practical point, Bitcoin moves quickly after being stolen, it may be split up and transferred around to different addresses before ending up at various off ramps where it is converted to fiat currency such as an exchange and this can happen in hours and if not hours certainly days, and the second reason is a legal issue because there is a requirement for much of the relief that you might get from a court that it thinks you have acted quickly and are in "hot pursuit" of the assets.

What has emerged in crypto case law to deal with misappropriated assets is a standard suite of relief that is sought from the court if it is possible to trace the misappropriated crypto to a particular exchange, and that is first and interim proprietary injunction and a worldwide freezing order to prohibit the fraudsters and the exchange from disposing of or dealing with this traceable crypto, and the second is a bankers trust disclosure order against the particular exchange to compel it to disclose certain information about the account holders behind the address where the crypto has ended up, and what I can do by way of illustration is just talk through a particular case that illustrates what this looks like in practice.

The particular case is called *Dainsz v Persons Unknown* and just a quick footnote, a lot of crypto cases are brought against persons unknown, this is a reasonably recent innovation in UK law where if you don't know the identity of the person who's defrauded you, the court will let you bring proceedings against persons unknown provided they can be described with sufficient particularity. So, in this particular case the claimant discovered a website called Matic Markets which encouraged users to invest in bitcoin through the website and the claimant did this and was led to believe that her bitcoin investments were doing very well and appreciating in value but when she requested to withdraw the bitcoin and the growth things went silent.

So, the claimant instructed a blockchain tracing expert to investigate what happened and that expert was able to trace the bitcoin to a crypto currency end wallet in a well-known crypto exchange and the claimant went to

	court and applied for that standard suite of relief that we've already discussed. Now the judgment is interesting because it has got some helpful text that really emphasises the need for victims of crypto fraud to act swiftly and in this case the claimant was commended for having done so, but even though they had done everything right in that regard, regrettably a significant amount of the misappropriated crypto had been dissipated by the time of the hearing. It is sad in this case where they did everything right, they still didn't get everything back. For completeness I'd note that this case allowed service outside of the jurisdiction, again a requirement there is that the claimant is in hot pursuit and it allowed for alternative service by email on both the website and by the exchange given the urgency. So, the court really will help you out in quite a big way if you're acting expeditiously.
Alice	And also that's a cue to remember to think beyond the obvious here. So, from an alternative perspective of the criminal law, if there is UK criminal jurisdiction which can be founded by things like, the property is here, or the harm occurred in the UK, or the suspect is in the UK, or the victim is in the UK, then you might be able to use the criminal law to assist you in that initial phase as well. So, under the Proceeds of Crime Act 2002, specifically section 41, there is a power to make what is called a restraint order, which operates much like a freezing order but specifically designed to protect assets against dissipation where there might well be a potential for a confiscation order at the end of criminal investigation and criminal proceedings. So, there is this power on the criminal courts as well to make a restraint order where certain conditions are met, some of which include that there is an ongoing criminal investigation or there are ongoing criminal proceedings. It's a reasonably commonly used power by "criminal investigators" or rather than private persons where there is a criminal investigation in relation to crypto assets. So, even as far back as 2018 this power was used to restrain about, at the time 975,000 worth of crypto assets which the court then ordered as well as being restrained to be converted into fiat currency and that to be restrained. So, the court has quite broad powers under this provision. The interesting thing about this is it can also be used for private prosecution, so a private prosecutor confirmed by the court in a case called Virgin Media v Zinga in 2014 said that private prosecutors can also have access to these proceeds of crime powers. So you mentioned a couple of times there Chris, blockchain tracing. How does that work and why is it important?
Chris	Great question Alice. Backing up, one of the key characteristic features of crypto currency, it's all available in the blockchain. In contrast with tracing fiat currency transfers where you have to identify the bank that it was transferred to, make a disclosure order, that may lead you to another bank and you gradually peel back the onion. On the blockchain you can see exactly where your crypto has gone in real time which has important implications for asset recovery. So, that means that if your bitcoin is misappropriated you can see exactly where it has gone. Now you can do this yourself, for example, in the case of bitcoin, there are websites like blockchain.com, where you see what's happened. But, what you really want to do is get an expert involved who has a lot of experience in interpreting the information you get on the blockchain, and they can add a lot of value because they can do things like trace between different blockchains and they can use various techniques to enrich the data that's available on the blockchain. For example, if it's transferred to a particular address, that's not tremendously helpful because you don't know much about it, but they can identify what kind of address it is by reference to other addresses that it's interacted with in the past, in a technique called clustering. So, because this is their bread and butter you really want to get them involved to maximise the chance of recovering anything. They are also extremely good when fraudsters take measures to disguise what they're doing. I have previously mentioned that it's rare that the bitcoin will just carry on in a linear path, it's often atomised and bounces between different addresses. One bit of tech that fraudsters may use is something called a mixer which essentially scrambles together the funds of multiple users to obfuscate the audit trail. An example of this is tornado cash, which operates on the theory of blockchain and it in very basic terms, what users can do is deposit sums of Ethereum that goes into a kind of black box and then they can withdraw it at a later stage. So, if person A, B and C all pay into this box, person A might later withdraw person C's Ethereum at a later point and what this process has done is broken on-chain link between the source and the destination address. One might feel pretty pessimistic about recovering crypto if fraudsters employ those kinds of measure but there is a glimmer of hope in a recent BVI case called ChainSwap v persons unknown which involved tornado cash. So, in this particular case the blockchain tracing expert identified that there were 24 transfers for a stable coin called DAI in a relatively short time window and then less than 24 hours later there were 24 transfers out of the same amount, minus a small commission payment, that went to a fourth wallet. The blockchain expert's report concluded that it was more likely than not, given the number and the size of

	payment in and out of tornado cash, and the relatively short time between those transfers, the inputs and outputs were linked, and the judge accepted that analysis and that ChainSwap had a good arguable case on that point. So, even if a mixer has been used it's not necessarily the end of the story.
Alice	And again, thinking from the different perspective, remember that the criminal law has been dealing with issues like this for years. If you think about the classic money laundering, it is quite common that you have layering and integration as part of the process of cleaning the money. So, the criminal law quite often looks to follow the trail of the asset through a number of different iterations and through a number of different types. So, Proceeds of Crime Act provides that you can trace the funds into mixed accounts, into other forms of property, provided that you can show that train, and if you can continue showing that train you can also trace it into the hands of new persons, including persons who might be connected with the fraud. What you can't do, is trace it into the hands of someone who is what we call, a bona fide purchaser for the value without notice. So, basically someone who has actually genuinely bought whatever it is without knowing any of the fraud and without being a party to it. But other than that the Proceeds of Crime Act does allow you to continue that tracing exercise, and there are a number of ways that that can happen. There are a number of different accounting principles that can be used. Most commonly it's first in first out, so taking that example that Chris just talked about where everyone puts A, B and C put a coin into a box and then take it out again, it wouldn't matter for the purposes of criminal law which coin went where provided you could show the linkage. If you can show the linkage between the fraud, and the coin, and the onward flow of funds, that would be enough for the criminal law. Again, it would involve quite a lot of technical expertise at this point because not only would you be needing the blockchain experts the trace the funds, you'd also at that point need forensic accounting services to prove that those funds, in the hands of a new person where for the purposes of furthering the original fraud and remained with that taint. But, if you could do that, again the criminal law is likely to look to help and indeed that is what commonly happens with what we would call normal criminal investigations, they usually do have to trace through a number of different iterations of property, and so the police services in the UK in particular have quite a lot of experience of tracking things into crypto currencies and NFTs and then continuing that trail on. How else does the UK law look to acquire misappropriated funds?
Chris	One possible option for which there has been no UK case law is something called a search order, which essentially allows you to access premises to preserve documents if you can demonstrate there is a risk of evidence being destroyed. Those orders, like freezing orders, are tough to get. How are they relevant to recovering stolen crypto assets? Well, backing up slightly and taking bitcoin as an example, one of the core concepts behind bitcoin are keys of which you have two types, a private key and a public key and they are roughly analogous to a pin code and bank account respectively. So, to transfer bitcoin on the blockchain you need to have your private key, i.e. your pin code and you need to know the public key of the recipient, i.e. their bank account and with those two things you can affect a transfer. Now private keys are considerably longer than a pin code which is great because it makes them hard to get, but it also means they are very, very difficult to remember and in practice one needs to store ones' private key in some way either in a specialised device called a hardware wallet or by simply writing in down in paper and those two things are often referred to as cold wallets. You might also store a private key as series of seed phrases which are used to generate a private key. So, if you find a piece of paper that says umbrella, coatrack, stars, moon, they might well be seed phrases for a private key and this might be relevant if you identify the hacker, and you want to examine their premises to see if you can seize any of these cold wallets. There is actually a recent Canadian case on precisely this point called Cicada 137 v Medjedovic which is also known as the teenage hacker case. The judgment for it isn't out yet but as I understand the facts, a particular hacker was outed, I think, because they used their user login one too many times, but anyway their identity became known, so the plaintiff brought a without notice application and raided the hacker's residence, it turned out the hacker was a teenage maths whiz and acquired the cold storage wallet devices and the passcodes. A final thought on this particular thing is, if you recover a cold wallet that doesn't mean that the crypto is necessarily safe and there are some comical stories of law enforcement getting this wrong in early days. The wallet will store the password but if your hacker has another copy of their private key they can still transfer their bitcoin somewhere else so what you actually need to do is use the private key to transfer the bitcoin to somewhere safe to prevent the hacker being able to use it.
Alice	And as you just mentioned there Chris, it's quite common for law enforcement officers to search and seize crypto currency either, as notable examples, everyone can think of headlines which have made global news

	of being the largest crypto seizure to date which seems to be trumped about monthly. But, in those cases they are all law enforcement officers. Unfortunately at this point there is no power for an individual, particularly acting in a private prosecution capacity, to conduct any form of search other than through the civil jurisdiction. There is no criminal law way which you can effect those searches, so it would just be as Chris described, going through the civil court process to obtain a search order. But it is quite common for authorities to search and to seize crypto assets and if you are in a position where you have advised authorities of the results up to a certain point and they are able to take over an investigation, it may very well be that they will conduct a search under the powers that are available to them to search and seize those assets. So, taking it forward a little bit, what about the next step. We've got as much information as we are going to get, how do you enforce it, how do you get that crypto back, or at least its value?
Chris	That's an interesting question, and one that has not actually been developed in case law very much. To my knowledge there is only one UK judgment actually dealing with crypto enforcement, which is the case of Ion Science which featured the first ever third-party debt order relating to a crypto currency theft. A third-party debt order allows whoever is owed money to take it from whoever currently has the money. So, in this particular case, which may be somewhat distinctive on its facts, the claimants successfully applied for a proprietary injunction and obtained freezing injunction and disclosure orders against Payward Limited which is a subsidiary of the Kraken Exchange. The disclosure order led to Payward disclosing that the entity behind the relevant account was something called Miriam Corp, and the disclosure showed that there were a certain amount of cash and crypto currency in that account. Now perhaps unusually it emerged that actually there was a debt owed by Payward to Miriam Corp and this led the high courts to make an interim third-party debt order, such that the claimant could recover from that debt what they had lost in the fraud. In the absence of a response from Miriam Corp that interim order was made final. But, more broadly the subject of enforcements against crypto assets is interesting and unfortunately, I probably don't have time to do full justice to it here, but I think we are only seeing the tip of the iceberg when it comes to crypto judgments generally, so I'm sure there will be further developments on it in due course. One final point that I should mention is that very soon I understand a judgment will be handed down involving a stolen NFT which is short for non-fundable token, and for those unaware this is a kind of unique cryptographic token, so unlike bitcoin which is interchangeable, this is one of a kind and you can think of them as essentially collectables, like trading cards. In this particular case the founder of the organisation, Women in Blockchain, Lavinia Osborne had two NFTs representing unique digital artworks that were removed without her consent from her digital wallet. Now she worked with a blockchain tracer who were able to locate the NFTs in two separate wallets in the NFT platform OpenSea, and then applied to court and obtained an injunction to freeze those assets and reveal the identities of the account holders and shortly afterwards OpenSea actually halted the sale of those NFTs. So, what we've been talking about doesn't just apply to crypto currencies, it also extends to tracing and recovering NFTs as well and the great thing about NFTs, unlike bitcoin which can be atomised and split up, you can't do that with an NFT, so you're chances of recovering it intact are much increased.
Alice	And that's true from the criminal law perspective as well because, of course, as soon as crypto became a thing it became a matter which could be a realisable property potentially. So, the courts have long ago determined that for the Proceeds of Crime Act and for the purposes of confiscation orders following conviction, of course a crypto asset is part of the persons potential property pool, so when you look at the confiscation proceedings following a conviction, so of course it does need to have some form of criminal conviction, you can then start to look at, well is this an asset which is part of their realisable property and part of the recoverable amount. Now those are very carefully conscribed matters which are dealt with under the Proceeds of Crime Act, and I will not bore everyone by going into them, but it is a relevant consideration that the most difficult part of enforcement for a confiscation order under the Proceeds of Crime Act is how much? because crypto currencies and NFTs fluctuate so widely in value, it is very difficult to ascertain exactly how much is actually available. So, one of the principles when you're looking at a confiscation order is that you have to ascertain how much property does the defendant actually have available to them, for the purposes of confiscation order. If you don't pay a confiscation order within a specified period of time you will receive a prison sentence in default, so it's incredibly important that there is a realistic snapshot of the persons actual property and therein lies the problem. How much is the crypto currency worth with the volatile market, when do you take this value, it is at the time the order is made, the crypto asset is acquired, is it at the time that the person goes to pay the order? The courts have side stepped the problem by requiring those crypto assets to be converted into fiat currency, and that is in fact what I spoke about earlier. The courts, when they go to restrain the crypto assets,

	have often required that those assets be transferred into fiat currency to be preserved for the purpose of a confiscation order should a criminal investigation end in conviction. So, that is a quick run through of the options available to a person who finds themselves part of the crypto scam. We mentioned at the start of this episode the incredible CFAAR network, so, Chris, how is that going and what is on the CFAAR horizon?
Chris	CFAAR has been doing well, we currently have around 1250 members. We've had a number of events so far and are looking to building on our early success by launching a number of foreign chapters. So, watch this space for developments on that, and then on the events front there are a number of things that we have in the pipeline. Our next big event, which we haven't announced yet, we are going to look precisely at enforcement, that is in the pipeline and hopefully there will be an announce on that soon. We're also launching a CFAAR breakfast club where people can meet with a brief keynote speaker and chat about the crypto issues of the day. The first one of those is on 1 June and at the time I speak there are still a few tickets left if people fancy it, and then finally we are trying to get some more webinar based content out and hopefully we will have an announcement about that soon, but it's likely to deal with the topic of mixers so building on what we've talked about here.

Alice	Unfortunately that's all we've got time for in this week's episode. Thank you again Chris for joining us. You can find Chris through RPCs website and you can find CFAAR on LinkedIn and through the show notes. If you have any questions for me or Chris or any topics you'd like us to cover in a future episode please do email us on taxingmatters@rpc.co.uk, we'd love to hear from you.
	RPC would like to thank podcast manager Josh McDonald. Original score was composed and produced by Inciter Music who also produced this podcast series. To hear a full uninterrupted version of our podcast theme go to Instagram @incitermusic and follow the link in bio.
Alice	And of course a big thank you to all of our listeners for joining us. If you like Taxing Matters why not try RPCs other podcast offering, Insurance Covered which looks at the inner workings of the insurance industry posted by the brilliant Peter Mansfield and available on Apple Podcast, Spotify, acast and our website. If you like this episode please do take a moment to rate, review and subscribe and remember to tell a colleague about us. Thank you all for listening and I'll talk to you again in two weeks.