THE HUMAN FACTOR
The limits of AI in investigations

CORRUPTION RECOVERY
Tracing stolen government funds

CRYPTO FRAUD
Crime, forensics and recovery

CDR
Commercial Dispute Resolution

www.cdr-news.com

April 2023

ESSENTIAL INTELLIGENCE:

Fraud, Asset Tracing & Recovery

Contributing Editor:
Keith Oliver
Peters & Peters Solicitors LLP

THE INTERNATIONAL ACADEMY OF FINANCIAL CRIME LITIGATORS

PETERS & PETERS

CDR Commercial Dispute Resolution

ESSENTIAL INTELLIGENCE:

Fraud, Asset Tracing & Recovery

EXPERT ANALYSIS CHAPTERS

JURISDICTION CHAPTERS

Singapore

Wendy Lin
WongPartnership LLP

Joel Quek
WongPartnership LLP

Jill Ann Koh
WongPartnership LLP

Leow Jiamin
WongPartnership LLP

I Executive summary

With around US$55.3 billion lost to scams worldwide in 2021 alone, fraud cases have undoubtedly increased in frequency, scope and complexity in recent years. Investment scams, and in particular those involving cryptocurrency, are growing rapidly, with Singapore being no stranger to this – in 2021, victims in Singapore lost at least S$633.3 million to scams, with investment scams racking up losses of S$190.9 million in total and accounting for the most amount of money stolen. However, the reality is that the majority of the culprits behind such scams are outside of Singapore, and in some cases, in locations that are completely unknown, limiting how much local law enforcement can do and rendering recovery of assets even more difficult.

In the face of such an unprecedented threat of fraud, exacerbated by the COVID-19 pandemic which has increased the speed at which people and businesses are operating online, Singapore, as with other jurisdictions, has had to respond rapidly on multiple fronts to strengthen enforcement against perpetrators. Apart from enhancing Singapore's legislative framework to increase regulatory oversight of the cryptocurrency industry, the Singapore Courts have also responded with ground-breaking decisions introducing novel tools to victims of fraud in their efforts to urgently locate, freeze and recover assets from fraudsters.

In this chapter, we discuss the options that victims have in respect of fraud, asset tracing and recovery, and the potential challenges they may face in Singapore.

II Important legal framework and statutory underpinnings to fraud, asset tracing and recovery schemes

It is often in fraud cases that it is imperative to act urgently to prevent fraudsters from disposing of or diminishing the value of the stolen assets. In recent

years, such assets would not uncommonly take the form of stolen cryptocurrency or NFTs. As cryptocurrency and NFTs are "*susceptible to being transferred by the click of a button, through digital wallets that may be completely anonymous and untraceable to the owner, and can be easily dissipated and hidden in cyberspace*" (as opined by the Singapore High Court in *CLM v CLN and ors* [2022] SGHC 46 ("***CLM***")), this heightens the need for tools to locate and freeze such assets pending any judgment being obtained against the fraudster.

In Singapore, the Courts have the power pursuant to section 18(2) read with paragraph 5 of the First Schedule of the Supreme Court of Judicature Act 1969 and section 4(10) of the Civil Law Act 1909 to grant injunctions and search orders in aid of a claimant. In the context of fraud and asset tracing, such orders would commonly be granted on an interim basis, and under the right circumstances, on an urgent basis without notice to the respondent or even before the originating process is issued.

In particular, the Courts can grant a proprietary injunction, which is aimed at preserving property over which a claimant has a claim and which allows the claimant to reclaim its ownership or possession of the property if it is ultimately successful in its claim against the wrongdoer.

The Courts also have at their disposal the *Mareva* injunction (following the eponymous case, *Mareva Compania Naviera SA v International Bulkcarriers SA* [1980] 1 All ER 213, and now known as the freezing injunction or freezing order) which aims to freeze the assets of the defendant either domestically or worldwide, without limitation to the stolen assets. Famously described as one of the "nuclear weapons" of civil litigation, a claimant seeking a *Mareva* injunction would have to show that there is a real risk that the defendant will dissipate his assets to frustrate the enforcement of an anticipated judgment of the Court, which requires proof on a much more exacting standard than when seeking an interim proprietary injunction (which requires demonstrating that the balance of convenience lies in favour of granting the injunction).

The difficulty in obtaining such injunction orders is compounded in a case where the actual identity of the fraudster is unknown and where the stolen asset, particularly cryptocurrency, has been routed through various channels, such as digital wallets and crypto exchanges, by the fraudster in an attempt to hamper tracing efforts, rendering the location of the asset unknown.

In such a situation, ancillary disclosure orders can be granted by the Courts to assist the claimant in locating the property, and in the case of a freezing injunction, to assist the claimant in determining the existence, nature and location of the defendant's assets, clarifying questions of title concerning the assets, and identifying the parties involved in the fraud as well as third parties to whom notice of the injunction should be given. A search order can also be sought to enable a claimant to enter the defendant's premises to search for, inspect and seize documents and materials to prevent the destruction of incriminating evidence.

A combination of these orders targeted at locating, preserving and recovering stolen assets were granted in two recent novel decisions of the Singapore High Court involving cryptocurrency and an NFT, in which the Court confirmed (for the first time, and following suit from other jurisdictions such as the UK and Malaysia) that civil proceedings can be commenced against unknown persons and injunctions obtained against them in order to prohibit the unknown persons from disposing of or diminishing the value of the stolen assets.

In *CLM*, an American entrepreneur discovered that Ethereum and Bitcoin up to the value of over US$7 million had been stolen from him and then dissipated through a series of digital wallets, which the Court observed as having appeared to have been "*created solely for the purpose of frustrating the [claimant's] tracing and recovery efforts, and which had either no or negligible transactions other than the deposit and withdrawal of the Stolen Cryptocurrency Assets*".

The claimant commenced proceedings against the persons unknown, and sought both a proprietary injunction and a worldwide freezing order to prohibit them from dealing with, disposing of, or diminishing the value of the stolen assets. In addition, the claimant sought ancillary disclosure orders against two operators of crypto exchanges for, among other things, information and documents collected by the crypto exchanges in relation to the owners of the accounts which received the stolen cryptocurrency. The Court granted the proprietary injunction and worldwide freezing order, the first of its kind granted in Singapore against the assets of persons unknown, as well as the ancillary disclosure orders.

In the decision of *Janesh s/o Rajkumar v Unknown Person ("CHEFPIERRE")* [2022] SGHC 264 ("***CHEFPIERRE***") released just several months later, the claimant brought an urgent application to Court for, among other things, an interim proprietary injunction prohibiting the defendant from dealing with an NFT, as well as permission to serve the Court papers on the defendant via Twitter, Discord and the defendant's cryptocurrency wallet address. The defendant's identity was not known to the claimant, but went by the pseudonym "chefpierre.eth".

The Singapore High Court held that while the forms in the Rules of Court 2021 in relation to commencing claims in Singapore require that the name and identification of a defendant be stated, so long as the description of the defendant is sufficiently certain to identify the persons falling within or outside of that description, strict compliance with the formality requirements in this respect was not required. In any case, even if the requirement for the defendant to be named was a strict one, the description of the defendant in *CHEFPIERRE* was

such that the Court would waive any such non-compliance with the Rules of Court.

The Court in *CHEFPIERRE* therefore allowed the claimant's application for permission to effect service via the various online platforms. In doing so, the Court clarified that it had the power to allow substituted service out of jurisdiction under the Rules of Court 2021, while also affirming previous Singapore decisions allowing substituted service to be effected *via* online platforms. This demonstrates the Singapore Courts' willingness to afford flexibility to claimants in commencing proceedings against fraudsters who may have an unknown identity or physical location, which is a critical tool in aid of recovery efforts against fraudsters.

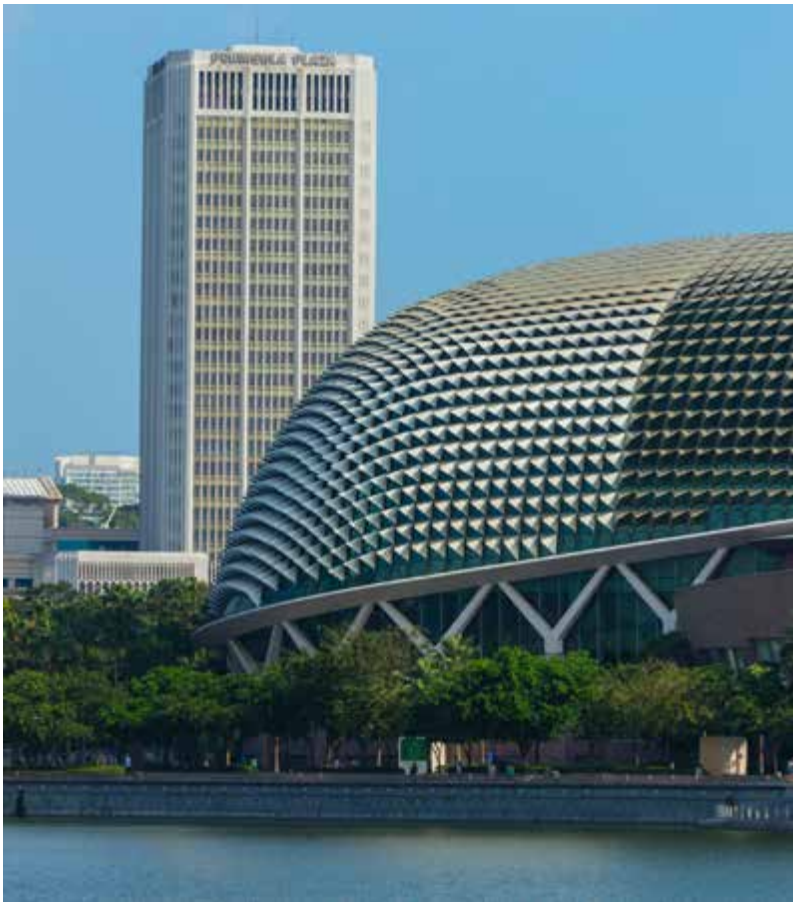
In addition to the above, section 18(2) read with paragraph 12 of the First Schedule of the Supreme Court of Judicature Act 1969 permits the Singapore Courts to grant a *Norwich Pharmacal* order (named after the House of Lords decision in *Norwich Pharmacal Co v Customs and Excise Commissioners* [1973] UKHL 6) against third parties requiring those third parties to disclose documents or information to the claimant to assist the claimant in identifying the person or persons who may be liable to the claimant.

The same statutory provisions also permit the Court to grant a *Bankers Trust* order (named after the English Court of Appeal decision in *Bankers Trust Co v Shapira* [1980] 1 WLR 1274). The purpose of a *Bankers Trust* order is to obtain disclosure of information from third parties, and are typically utilised in claims for fraud where a claimant seeks confidential documents from a bank (or, in recent cases, crypto exchanges) to support a proprietary claim to trace assets.

In this regard, while the English High Court has confirmed that *Bankers Trust* orders can be served on entities (such as crypto exchanges) outside the jurisdiction (see, for example, *LMN v Bitflyer Holdings Inc. and others* [2022] EWHC 2954 (Comm)), the Singapore Courts have yet to rule on this. In *CLM*, for example, this issue did not arise as although *Bankers Trust* orders were sought against two crypto exchanges incorporated overseas, these defendants also had operations in Singapore. Further, the Singapore High Court in *CLM* declined to consider whether a *Bankers Trust* order should be granted, as the crypto exchanges were already parties to the proceedings, and therefore were not non-parties. If Singapore is to remain at the forefront of dispute resolution for fraud victims seeking redress, it would be helpful for the Courts to adopt a similar, more permissive stance to issuing *Bankers Trust* orders to third parties overseas, particularly when such third parties in crypto asset disputes are increasingly based outside the jurisdiction.

III Case triage: main stages of fraud, asset tracing and recovery cases

Time is always of the essence. The first step is to ensure that as much information and evidence is gathered in respect of the fraud in order to formulate a legal and asset recovery strategy. This must be done swiftly and decisively as fraudsters look to erase or hide evidence of their wrongdoing and avoid being identified. It is therefore important to involve technical experts at an early stage to deploy



technological tools to assist in evidence gathering and recovery, as well as to pick up on trails left behind by the fraudsters that may yield useful information and evidence.

As a second step, the claimant should decide on the jurisdiction(s) where the claim should be brought against the wrongdoer, and how this impacts the claimant obtaining injunction, search and/or disclosure orders. Where the fraud is cross-border in nature, it is especially critical for the claimant to have an appreciation of how the legal mechanisms available in various jurisdictions can complement one another.

Where multiple jurisdictions are available, it would also be necessary to consider the question of whether proceedings should be commenced concurrently in each of the available jurisdictions, or whether more advantages can be gained in commencing proceedings in one main jurisdiction, and thereafter enforcing the orders obtained in that jurisdiction in the other available jurisdictions.

In this regard, it is worth noting that the Singapore Courts are widely supportive of foreign proceedings and have broad powers to grant interim relief in aid of such proceedings. In practice, the Singapore Courts are also generally willing to give effect to injunctions or other orders obtained outside Singapore, by granting similar orders to that effect.

For instance, the Singapore Courts can grant freezing injunctions in aid of foreign proceedings so as to assist the claimant in ensuring that if he is successful in those proceedings, he would have assets in Singapore over which to enforce the foreign judgment. In *Bi Xiaoqiong v China Medical Technologies, Inc (in liquidation) and anor* [2019] 2 SLR 595, the Court held that its power to do so is subject to at least two conditions: that the Court has *in personam* jurisdiction over the defendant; and the claimant has a reasonable accrued cause of action against the defendant in Singapore. Importantly, there is no requirement that the Singapore proceedings have to terminate in a judgment rendered by the Court that issued the injunction, and the freezing injunction can be granted even where the Singapore proceedings are stayed in favour of foreign proceedings.

Following this decision, by amendments which took effect in 2022, provisions were introduced in the Singapore Civil Law Act 1909 to enable the General Division of the High Court of Singapore to grant any type of interim relief (as long as it also has the power to grant such relief in proceedings within its own jurisdiction) in aid of foreign Court proceedings, *even if* there are no substantive proceedings in Singapore. This is commonly known as "free-standing" interim relief. With these amendments, the Court's powers to grant relief in aid of foreign Court proceedings appear to have been broadened markedly. However, as there are yet to be any reported decisions of the Singapore Courts on these new provisions, how the Courts will exercise this power (particularly as the amended provisions still permit the Court to refuse to grant relief if it considers that its lack of jurisdiction over the subject matter of the proceedings would make it inappropriate to do so) remains untested.

Further, by amendments to the Reciprocal Enforcement of Foreign Judgments Act 1959 ("**REFJA**"), which came into effect in 2019, foreign interlocutory orders such as freezing orders and foreign non-money judgments obtained in foreign gazetted territories can be enforced in Singapore. Such amendments plug a long-standing gap as freezing orders (not being "final and conclusive" judgments) were not previously capable of enforcement under the Act. At the moment, these amendments apply only to judgments from the superior courts of Hong Kong that are registrable under the REFJA. With the recent repeal of the Reciprocal Enforcement of Commonwealth Judgments Act 1921 on 1 March 2023, Singapore's

legal framework for the statutory recognition and enforcement of foreign judgments in civil proceedings is now streamlined and consolidated such that foreign judgments issued by stipulated courts from the United Kingdom, Australia, New Zealand, Sri Lanka, Malaysia, Windward Islands, Pakistan, Brunei, Papua New Guinea and India are also registrable under the REFJA. Currently, only money judgments that are final and conclusive as between the parties to the judgments from these Courts are registrable under the REFJA, but it is expected that this will be expanded to be in line with judgments from Hong Kong.

Once proceedings are commenced, the third step involves obtaining the relevant injunctions, search orders and/or disclosure orders as elaborated on in the previous section. In this regard, claimants must be mindful that injunctions obtained in Singapore are usually accompanied by undertakings. For instance, before a worldwide freezing injunction is granted by the Singapore Courts, it is usual that the claimant undertakes to seek permission before (1) enforcing that injunction any other jurisdiction, or (2) starting proceedings against the defendant in any other jurisdiction.

More information about the wrongdoer and the wrongdoer's assets will often be obtained at this stage. It is critical to reassess the overall legal and asset tracing strategy as new information becomes available to ensure efficacy and efficiency in the conduct of legal proceedings.

For instance, the claimant may be able to identify other wrongdoers against whom recourse could be had. This may necessitate further parties being added to existing legal proceedings, either as defendants or parties against whom further orders need to be sought against. Indeed, this was the case in *CLM*, where as a result of the claimant's further investigations and disclosure by the second and third defendants, the claimant identified two other persons who were involved in the transfer of assets which were traceable to the crypto assets which were the subject matter of the claim, and proceeded to join them as fourth and fifth defendants in the Singapore proceedings.

Where the legal and asset tracing strategy is conducted effectively, this may result in the wrongdoer being more amenable to enter into a settlement on terms favourable to the claimant. This usually results in significant time and costs savings for the claimant. Where there is no settlement of the dispute, the proceedings will either proceed to trial (if the defendant contests the proceedings), or a judgment would be entered in default (if the defendant does not contest the proceedings).

Once a judgment is obtained against the defendants, steps to execute the judgment against the assets of the defendants can be taken. This process will be significantly streamlined and simplified if the locations of the defendant's assets are known to the claimant and the requisite injunctions have already been obtained.

IV Parallel proceedings: a combined civil and criminal approach

While it is possible to pursue parallel civil and criminal proceedings against fraudsters in Singapore, from an asset recovery perspective, civil proceedings play a more impactful role. This is a function of the different intended purposes and outcomes of criminal and civil proceedings – criminal proceedings are aimed at deterrence and/or criminal punishment, while the objective of civil proceedings is to provide compensation and/or recovery of assets to the claimant.

For example, in a recent decision on a disposal inquiry in *Lim Tien Hou William v Ling Kok Hua* [2023] SGHC 18, the Singapore High Court determined that in a contest between two individuals who were both victims of cryptocurrency fraud, the stolen asset should be returned to the party who was the lawful possessor of the asset at the point of seizure. In reaching this decision, the Court clarified that its ruling was based on provisions of the Criminal Procedure Code, and had no effect on a Civil Court. Parties are thus free to commence civil proceedings to assert their rights.

Defendants in civil proceedings may also try to use the fact that they are subject to criminal proceedings as a means to delay the civil proceedings brought against them. This was precisely the scenario in the Singapore High Court case of *Debenho Pte Ltd and or v Envy Global Trading Pte Ltd and Ng Yu Zhi* [2022] SGHC 7. Mr Ng Yu Zhi ("**NYZ**") sought a stay of civil proceedings brought against him for, among other things, fraudulent misrepresentation, on the basis that he also faced criminal charges arising out of the same facts (alleged fraud surrounding an investment scheme involving physical nickel trading). Two of the criminal cheating charges brought against NYZ were in respect of the claimants in the civil suit. NYZ argued, among other things, that he enjoys the right of silence and the privilege against self-incrimination, both of which will be infringed if the civil suit is not stayed, and he would suffer prejudice if the civil suit is not stayed because of the burden of having to prepare for both sets of proceedings concurrently.

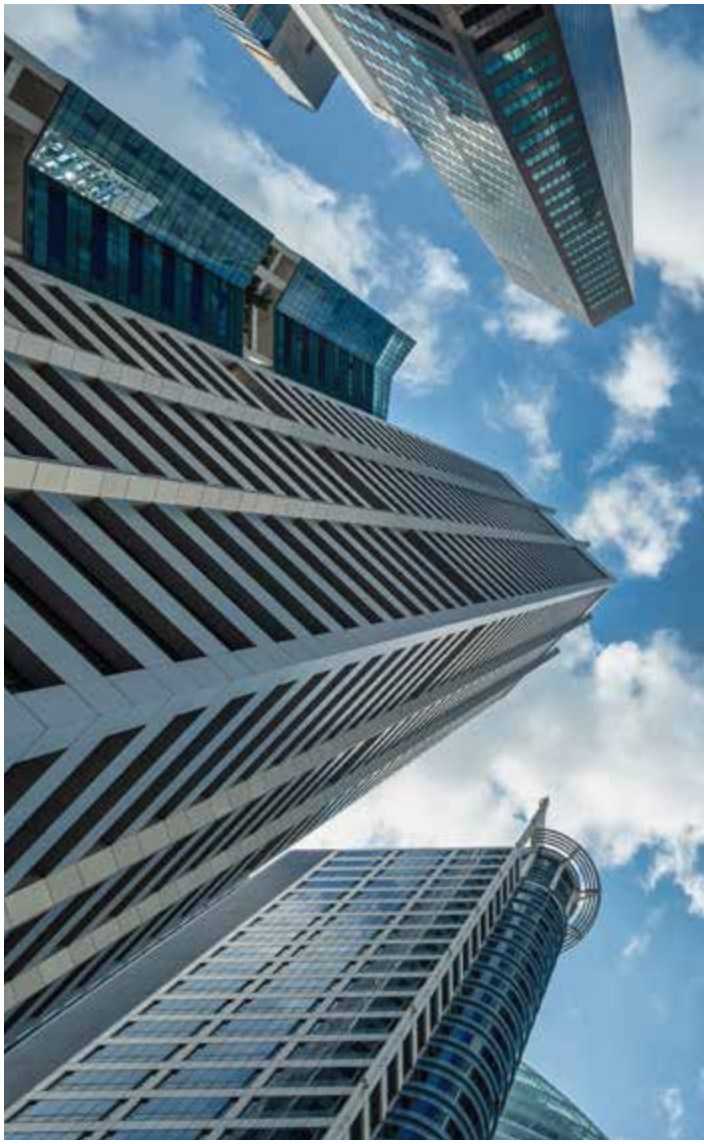
The High Court dismissed the stay application because it was insufficient for NYZ to simply invoke his right of silence and privilege against self-incrimination, both of which are not automatically engaged merely because he has been called upon to defend himself in a civil action. NYZ failed to show how requiring him to defendant himself in the civil suit will give rise to a real (and not just notional) danger of prejudice. In particular, the High Court held that section 134(2) of the Evidence Act 1997 precludes any incriminating answers that NYZ may give under cross-examination in the civil suit from being proved against him in the criminal trial.

However, claimants should bear in mind the possibility of such arguments being deployed by wrongdoers to delay civil proceedings against them, especially where the wrongdoer is able to show a real danger of prejudice.

V Key challenges

One key challenge faced by claimants investigating frauds and trying to recover stolen assets is the lack of information. This is especially concerning when a wide array of tools is now available to fraudsters to mask their identity and location, as well as to move stolen assets quickly and seamlessly, making asset tracing and recovery efforts against the wrongdoer a costly and time-consuming exercise for the claimant.

In the context of crypto fraud, identifying where the stolen crypto assets reside on the blockchain (in a crypto exchange) or where it was last known (before being transferred to a cold wallet) is relatively straightforward, with the legal and technological avenues for seeking redress becoming better known. That is not to say the process of asset tracing



and recovery is not without its difficulties, given the ease of transferring and/or mixing the crypto assets across multiple accounts and parties, which only adds to the costs and time taken to obtain recovery against the wrongdoer. However, the path to recovery has been made increasingly less thorny by, among other things, the Singapore Courts' move to allow proceedings to be commenced against unknown defendants and for orders to be obtained against them.

VI Coping with COVID-19

The pandemic has created many unprecedented firsts, including in the legal industry. The Singapore Courts have responded efficiently, implementing virtual hearings in place of physical attendance in court. In the context of urgent hearings (for, *e.g.*, applications for an interim proprietary injunction or freezing injunction), the use of virtual hearings has expedited the process and allowed urgent matters to be dealt with far more efficiently than ever before.

While Singapore has largely eased COVID-19-related restrictive measures and reopened its borders, virtual hearings are still routinely conducted, as the Singapore Courts and users recognise their increased efficiency and convenience as compared to physical in-person hearings – especially for urgent interim applications.

VII Cross-jurisdictional mechanisms: issues and solutions in recent times

Fraud and asset tracing are increasingly cross-border in nature. The fraud is either in itself cross-border, or the asset stolen is usually moved overseas. Therefore, as discussed above, it is critical to devise a multi-jurisdictional strategy in fraud and asset tracing which involves identifying the potential jurisdictions involved, the various positions each jurisdiction takes in respect of injunction and disclosure orders, and whether enforcement of such orders granted by a foreign Court poses a challenge.

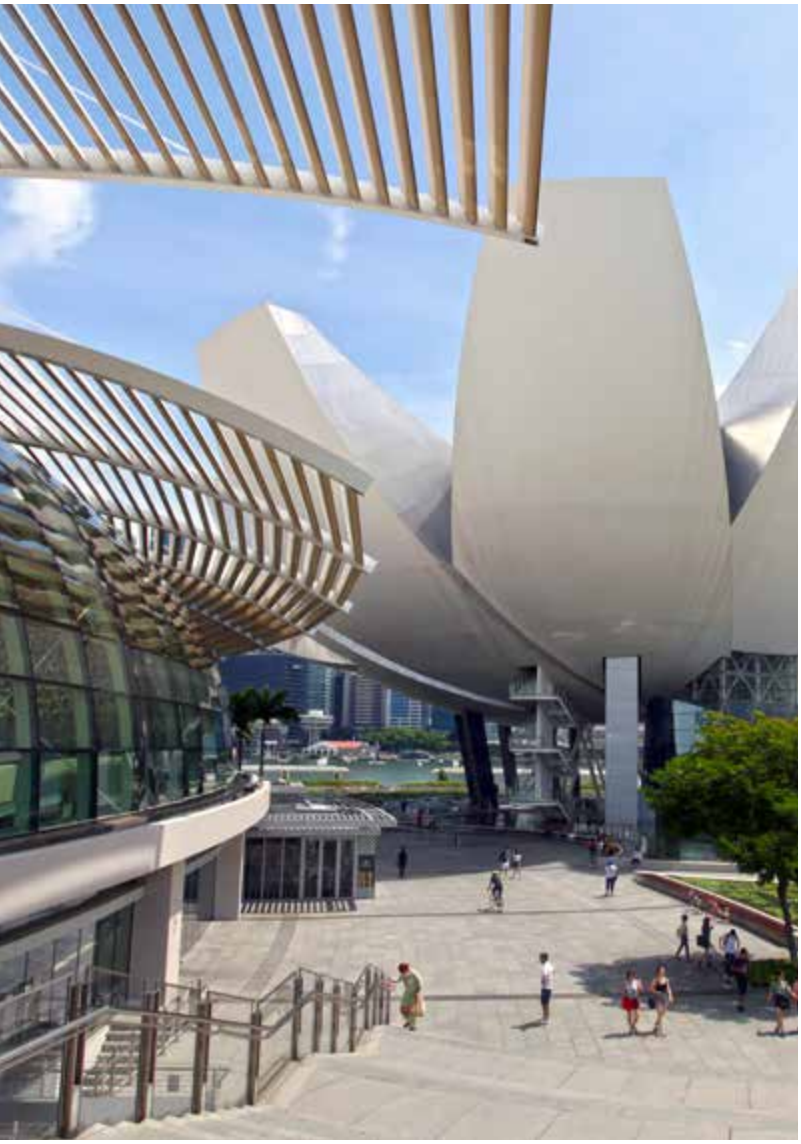
The challenges that arise from cross-border fraud and asset tracing are nonetheless alleviated by the Singapore Courts' willingness to recognise and grant relief in support of foreign proceedings, making Singapore an attractive jurisdiction for claimants to consider when coming up with their legal and asset tracing strategy.

VIII Using technology to aid asset recovery

It has been discussed that a potential claimant would likely have to work with technical experts to preserve as much technical evidence as possible as most fraud today would involve some digital or technical aspect. Fraudsters would also not shy away from using tools readily at their disposal to hide their identity and location, and the location of the stolen assets.

Artificial intelligence (AI) has been touted as one of the new tools to be deployed in asset tracing. AI may be able to complete in seconds what may take a human months or years to do, and has been used in systems designed to trigger alerts when transactions that have a high risk of being fraudulent are detected, or in systems touted as being able to trace, within a very short period of time, communication between email addresses belonging to persons of interest and their bank accounts. The fact that AI is able to process voluminous and complex data autonomously to identify trends and patterns without (or with very minimal) human intervention is a significant advantage that claimants should take advantage of.

Nonetheless, there remains a question as to how reliable AI results are. In the long-drawn litigation in the UK in *Bates v Post Office Ltd (No 6: Horizon Issues) Technical Appendix* [2019] EWHC 3408 (QB), an IT system had detected unexplained discrep-



ancies in various accounts. That led to successful private prosecution of more than 900 ex-employees for theft, false accounting and/or fraud. The system was later found to contain software bugs, errors and defects "*far larger number than ought to have been present in the system if* [the system] *were to be considered sufficiently robust such that they were extremely unlikely to be considered the cause of shortfalls in branches*". Serious doubts were then raised in respect of the reliability of such evidence. It therefore remains to be seen the extent to which AI can reliably assist in asset tracing and recovery.

IX Highlighting the influence of digital currencies: is this a game changer?

The steps to be taken in respect of fraud concerning cryptocurrencies and tokens are generally the same as traditional assets.

There remains one aspect of uncertainty which would benefit from more jurisprudence in common law – are digital currencies considered "property" in the eyes of the law? It has been long regarded that there are principally two categories of property: (a) a "chose in possession" (referring to physical assets, which digital currencies, such as Bitcoin, are not); and (b) a "chose in action". This categorisation arises out of a dissenting English Judge's finding made in 1885 (*Colonial Bank v Whinney* [1885] 30 Ch.D 261).

We consider a hypothetical example of one depositing monies with a bank. Prior to the deposit, the monies exist in the form of physical cash, which is a "chose in possession". Once the monies are deposited they no longer have a physical presence, and they are a "chose in action" (where the proprietary right arises from the fact that action can be taken against the bank to enforce your rights in the monies deposited).

Unlike monies deposited with a bank, cryptocurrencies reside on the blockchain (which are pockets of data replicated across the network). In the case of a decentralised network, there is no particular issuer (*i.e.*, nothing equivalent to a central bank). Strictly speaking, therefore, there is no one against whom an action can be taken to enforce the rights in the crypto asset.

What about the digital wallets opened with crypto exchanges? Do they not operate similarly to banks? What is in the digital wallet, however, is not the cryptocurrency itself, but the private keys allowing one to access or control the cryptocurrency residing on the blockchain. It is therefore not necessarily the case that a proprietary right arises against the crypto exchanges in respect of cryptocurrency residing on the blockchain simply because the crypto exchanges hold digital wallets. Further, not all cryptocurrencies are stored with crypto exchanges; many choose to create cold wallets (*i.e.*, devices that are disconnected from the internet) for added security.

The Singapore High Court has considered that cryptocurrencies (such as stolen Bitcoin and Ethereum) fall within the classic *Ainsworth* definition of property (namely, that it must be "*definable, identifiable by third parties, capable in its nature of assumption by third parties, and have some degree of permanence or stability*") and were "*capable of giving rise to proprietary rights, which could be protected via a proprietary injunction*" (in *CLM*). The same position was taken in respect of NFTs (in *CHEFPIERRE*).

This is similar to the position that other commonwealth Courts have adopted at present. The New Zealand Courts opined that while it has long been regarded that there are two categories of property, that in itself is a matter of categorisation and does not limit what can be recognised as "property", and the categorisation itself would not lead a Court to conclude that cryptocurrencies are not property (*Ruscoe v Cryptopia Limited (in liquidation)* [2020] NZHC 729). The UK Courts have also commented that it would be "*fallacious to proceed on the basis that the English law of property recognises no forms of property other than choses in possession and choses in action*" (*AA v Persons Unknown who demanded Bitcoin on 10th and 11th October 2019 and ors* [2019] EWHC 3556 (Comm)).

X Recent developments and other impacting factors

Singapore is in the epicentre of combatting commercial fraud, cyber scams and crypto fraud. Other than civil proceedings which have been discussed above, industry-specific efforts have been made to curb such fraud and scams.

For instance, following a widespread SMS phishing attack impersonating a bank in Singapore in 2021 that resulted in $13.7 million lost in days by at least 790 victims, the Association of Banks in Singapore Standing Committee on Fraud worked with the Monetary Authority of Singapore and Singapore Police Force to coordinate the industry's continuous anti-scam efforts in the banking industry.

Legislatively, regulations are continually being introduced to address cryptocurrency frauds. One example is the Singapore Payment Services Act 2019 that was amended in 2021 in a bid to strengthen the laws that govern digital payment tokens. In particular, the scope of the Act was expanded to confer on the Monetary Authority of Singapore powers to regulate service providers of digital payment tokens ("**DPTs**") that facilitate the use of DPTs for payments, and may not possess the moneys or DPTs involved (termed as Virtual Assets Service Providers, or "**VASPs**").

The Financial Services and Markets Bill was also introduced in 2022 to build upon and enhance the existing regulation of VASPs. Recognising the need to mitigate the risk of regulatory arbitrage (where no single jurisdiction has sufficient regulatory hold over a specific VASP due to the internet and digital nature of its business), such VASPs which provide digital token services outside of Singapore are now regulated as a new class of Financial Institutions, with licensing and ongoing requirements to ensure that the Monetary Authority of Singapore has adequate supervisory oversight over them.

While such regulatory steps have been taken in a bid to deter and prevent fraud before it can even take root, ultimately, civil remedies are still the main means to counter the effects of fraud.

That being said, while the landscape of fraud has been irretrievably altered, contributed in no small part by the COVID-19 pandemic, Singapore continues to rapidly evolve to adapt to these changes, offering new and novel tools to victims of fraud to equip them to face these challenges head on. CDR

Headquartered in Singapore, **WongPartnership LLP** is a market leader and one of the largest law firms in the country. We offer our clients access to our offices in China and Myanmar, and in Abu Dhabi, Dubai, Indonesia, Malaysia, and Philippines, through the member firms of WPG, a regional law network. Together, WPG offers the expertise of over 400 professionals to meet the needs of our clients throughout the region.

Our expertise spans the full suite of legal services to include both advisory and transactional work where we have been involved in landmark corporate transactions, as well as complex and high-profile litigation and arbitration matters. WongPartnership is also a member of the globally renowned World Law Group, one of the oldest and largest networks of leading law firms.

At WongPartnership, we recognise that our clients want to work with the best. As a partnership of exceptional individuals, we are committed in every way to make that happen.

www.wongpartnership.com

Wendy Lin is a Partner in the Commercial & Corporate Disputes and International Arbitration Practices at WongPartnership LLP.

Her active practice spans across a wide array of high-value, multi-jurisdictional and complex commercial, fraud and asset recovery disputes before the Singapore Courts. She is also currently serving her third term as Co-Chair of the YSIAC Committee, and is a member of the Singapore Academy of Law's Law Reform Committee.

Wendy has consistently been recommended in legal publications for her dispute resolution work; with sources noting she is "*a phenomenal and utterly compelling advocate who is extremely quick on her feet and has unrivalled analytical skills*", and "*a first-class advocate, with the unparalleled ability to cut through numerous complex facts, extract the winning arguments, and to convey them effectively, with absolute charm and ease*".

She has also earned the rare distinction since 2020 of being selected as a Global Leader by *Who's Who Legal* in three practice areas (Litigation, Arbitration and Asset Recovery), and as a Thought Leader in Commercial Litigation and Asset Recovery since 2022.

wendy.lin@wongpartnership.com

Joel Quek is a Partner in the Commercial & Corporate Disputes Practice at WongPartnership LLP.

His main areas of practice are in litigation and arbitration, involving commercial, corporate, shareholder and employment disputes across a range of sectors including energy, commodities, finance, transport, construction and healthcare. Joel also has an active investment treaty arbitration practice, acting for both private investors and State parties.

Prior to entering private practice, Joel served as a Justices' Law Clerk to the Chief Justice and Judges of the Singapore Supreme Court. His experience also includes a placement with Fountain Court Chambers in London where he worked with barristers and King's Counsel on a variety of matters in the English Commercial Courts. In addition to his practice, Joel teaches trial advocacy in the National University of Singapore and previously taught commercial conflict of laws in the Singapore Management University.

joel.quek@wongpartnership.com

Jill Ann Koh is a Partner in the Commercial & Corporate Disputes Practice at WongPartnership LLP.

She has an active court and international arbitration practice in a wide range of complex, high-value and multi-jurisdictional disputes, including in the areas of corporate and commercial, shareholder, investment and contractual disputes. She also regularly advises on a broad range of legal issues including matters relating to corporate governance and compliance, tenancy and employment.

Jill graduated from the Singapore Management University, which she represented in the Philip C. Jessup International Law Moot and the Willem C. Vis International Commercial Arbitration Moot. She is admitted to the Singapore Bar.

jillann.koh@wongpartnership.com

Leow Jiamin is a Partner in the Commercial & Corporate Disputes Practice at WongPartnership LLP.

Her practice involves a wide range of court and arbitration matters, ranging from commercial and corporate, cross-border, fraud, asset recovery, to intellectual property disputes. She is also fluent in Mandarin and regularly acts for Mandarin-speaking and Chinese clients.

Jiamin currently serves in the Cybersecurity and Data Protection Committee, Intellectual Property Committee of the Singapore Law Society, as well as the Asset Recovery Next Gen Committee. She was mentioned in *The Legal 500* (Asia Pacific) in 2019, and *IAM Patent 1000* (Singapore) in 2020.

She was placed Joint 4th in the 2014 Singapore Bar Examinations, and was awarded two distinctions (Intellectual Property Law and The Singapore Institute of Legal Education's Prize for the Top Student in Family Law).

Jiamin graduated with a Bachelor's degree in Engineering from Nanyang Technological University and obtained a *Juris Doctor* from Singapore Management University. Jiamin is admitted to the Singapore Bar.

jiamin.leow@wongpartnership.com