CDR
Commercial Dispute Resolution

BLOCKCHAIN AND FRAUD
Facing up to technology challenges in asset tracing

INTERNATIONAL RECOVERY
Using criminal law tools in cross-border cases

COUNTRY ANALYSES
Guides to law and procedure in key jurisdictions

www.cdr-news.com Spring 2020

ESSENTIAL INTELLIGENCE:

Fraud, Asset Tracing & Recovery

Contributing Editor:

Keith Oliver
Peters & Peters

THE INTERNATIONAL ACADEMY OF FINANCIAL CRIME LITIGATORS
PETERS & PETERS
ICLG.com

FROM THE EDITOR

Welcome to the first Essential Intelligence edition of *CDR*.

There is perhaps no topic whose development is being watched more closely by clients than that of fraud and asset tracing.

It is an era in which the banking and finance sectors are being transformed by new technology, when there are seemingly new stories of fraud and cyber breach every week, and one in which regulators are taking a more aggressive stance on corporate behaviour and governance.

In the UK, that regulatory scrutiny is seen in the growth of 'failure to prevent' offences, and the introduction of deferred prosecution agreements and the Senior Managers and Certification Regime, but there are similar enforcement tools developing in other countries, particularly as the US Department of Justice is increasingly exporting justice to other jurisdictions.

As such, there has never been greater pressure on lawyers to provide their clients with the tools to protect themselves from fraud and to recover lost assets, and I hope this guide will go some way to shining a light on the development of this practice area.

I would like to extend my sincere thanks to Keith Oliver and Peters & Peters for their support and assistance with this title. The next edition, which will tackle Belt and Road Initiative disputes, will be out in mid-2020.

Andrew Mizner
Editor
Commercial Dispute Resolution

CDR Commercial Dispute Resolution
ISSN: 2633-755X

PUBLISHED BY
Global Legal Group Ltd
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
www.glgroup.co.uk

glg global legal group

EDITOR
Andrew Mizner
andrew.mizner@glgroup.co.uk

PUBLISHER
George Archer
george.archer@glgroup.co.uk

MARKETING MANAGER
Rachel Williams
rachel.williams@glgroup.co.uk

DISTRIBUTION MANAGER
Mark Carroll
mark.carroll@glgroup.co.uk

CHIEF MEDIA OFFICER
Fraser Allan
fraser.allan@glgroup.co.uk

CHIEF COMMERCIAL OFFICER
Florjan Osmani
florjan.osmani@glgroup.co.uk

Cover image by iStock.com. All author portraits courtesy of the individuals' firms/companies. All other images by iStock.com, except where indicated.

PRINTED BY
Stephens and George Print Group
Goat Mill Road, Dowlais
Merthyr Tydfil CF48 3TD
www.stephensandgeorge.co.uk

TABLE OF CONTENTS

INTELLIGENCE BRIEFINGS

COUNTRY ANALYSES

PREFACE

It is with great pleasure that we welcome you to the first edition of the *CDR* Essential Intelligence series. Peters & Peters Solicitors LLP has been delighted to serve as the contributing editor to the first publication in this series. This is an all-encompassing and comprehensive guide to the practice of global fraud, asset tracing & recovery litigation.

It has been an eventful 12 months in the international fraud arena. Crowe's *2019 The Financial Cost of Fraud Report* indicates that fraud has cost the global economy £3.89 trillion in the last year, with losses having risen by 56% in the last 10 years. A key international contributing factor to this figure is the rise of cyber criminality and abuses. According to the *PwC Global Economic Crime Survey*, 26% of global frauds now have some form of cybercrime element to them. This is unsurprising with the introduction of disruptive technologies such as blockchain, cryptoassets and the Internet of things. It is now vital that we adapt to the wave of change impacting our sector, lest we are left behind by 'the march of technology'. However, this is but one of the numerous developments that have played a part in sculpting the fraud, asset tracing & recovery landscape as we head into 2020.

Therefore, the intention of this guide is to provide a clear and cogent overview of the practice of fraud, asset tracing & recovery litigation in varying countries around the world, working towards global innovation and best practice through the sharing of knowledge and expertise. We would like to take this opportunity to thank the tireless efforts of our contributing authors, who include some of the world's leading law firms, a wide range of expert practitioners, barristers' chambers and forensic accountants. Their generous contributions to this project have created an invaluable holistic picture of the international legal response, which we hope will be useful for our readers both now and in years to come.

Keith Oliver
Head of International
Peters & Peters LLP

With banking in the middle of a blockchain revolution, would-be fraudsters, asset tracing professionals and lawyers are facing up to the future

Navigating the blockchain challenge

Andrew Mizner
Commercial Dispute Resolution

In little over a decade, blockchain has begun to transform the world of international finance. While the revolution is still in its early days and the applications of blockchain are still being explored, as companies of all sizes explore how to use cryptocurrencies to raise funds and blockchain to offer improved services, there are also new opportunities to steal and conceal assets.

To date, blockchain has had qualities which appeal to those on either side of the legal divide. Its anonymity appeals to those who want privacy for their dealings; on the other hand, the transparency of transactions gives investigators some insights into where the money is going, up to a point at least.

"Externally an investigator can view the blockchain, get into it and see all the transactions that happen to it. And then to counter that, there are the mixers into which bitcoins go and are completely plunged around and anonymised," says **Matthew Rees**, a director at **Forensic Risk Alliance**.

Investigators are constantly "fighting against the means through which that transparency is obscured", he explains. "Exchanging bitcoins, so you break the link between the funds that need to be hidden away and the funds as they are in their current state."

This game of cat and mouse creates challenges for investigators, says **Keith Oliver**, head of international at **Peters & Peters**: "The problem with the legal aspects of the technology is that if you look at joining up the dots that underpin the way in which the whole mechanism works, it is not impossible, but is incredibly challenging to chase and to be able to trace the elements in the chain that give rise to the transactions. And there is no joined up international jurisdiction for the purpose of dealing with it."

Although there have been some high-profile blockchain-related frauds, including the Gerald Cotten/Quadriga scandal, blockchain fraud has

not yet taken off, he argues: "It is only when we get to a stage where someone actually tries to buy an asset and the asset isn't delivered, that you will have to look at the legal structure and see whether you can trace it. What is the underlying contract that brings the two parties together and the governing law? That's the starting point."

As Rees says, none of this new technology makes fraud easier, "it is just another route".

"Initially, the worry for the authorities was that it would be so easy to flip money around in a completely anonymous way. It hasn't become the massive problem that we thought it would be."

This is partly due to the fact that there are still plenty of opportunities to exploit the traditional banking system and as Rees points out, the fraudsters can themselves be ripped off through the same vulnerabilities which they exploited in the first place.

The underlying technology behind blockchain means that it should theoretically be unhackable, because it is an open platform which does not rely on a single financial intermediary to initiate or validate transactions. "Instead it gives power back to the people, in an idealistic sense, but what that really means is that every network participant to a specific blockchain is aware of every single transaction that is going on," explains Oliver's colleague, legal researcher **Amalia Neenan**.

That is a long way removed from traditional banking and transactions. "If this were to be harnessed properly, appropriately, and in the correct regulatory environment, then the potential for this is magnificent and it could hopefully revolutionise how we transact in the future, we have just got to iron the kinks out at the moment," she enthuses.

Old wine, new bottles

While the means by which money can be moved may be changing, the basic principles remain the same and Oliver runs off a list of historical and current frauds and data violations, including phishing emails, the hacking of Jeff Bezos' phone and how the first Ponzi schemes manipulated postal technology of their time.

To a certain degree, blockchain is a victim of how it is perceived: "Everyone thinks it is this new thing that we all need to fear, and to an extent there should be a level of caution with that," says Neenan, "but it is not necessarily a unique form of fraud itself, merely the platform has changed".

It is "old wine, new bottles", agrees Rees. "The people who want to move the money want to achieve the same thing, but they just use new technologies to do it." The principles of putting gaps between the source of the money and the intended recipient remain the same and blockchain-based financial services or cryptocurrency exchanges are another means of achieving that.

It has "absolutely" got easier to move money illicitly, says Oliver. "The question is this: how secure can any system be, for the purposes of engaging in any sort of financial transaction?"

Changing tools

Lawyers, accountants and regulators should be finding new ways to trace assets, but although some of the bigger players are developing new tools, opinion varies about how much progress there has been to date.

Rees argues that it is not the methods that have changed, but the capacity to do so. He describes it as "a little arms race", which he goes on to qualify: "It is not rocketing, it is a gradual hill of our power versus the ingenuity of people moving money around."

That means using more powerful computers and more advanced algorithms "to build bespoke, metaphorical pictures, build the understanding of what transactions have done and use that understanding to look for similar forms of activity", he explains.

Karyn Harty, a partner with **McCann**

To date, blockchain has had qualities which appeal to those on either side of the legal divide. Its anonymity appeals to those who want privacy for their dealings; on the other hand, the transparency of transactions gives investigators some insights into where the money is going, up to a point at least

Fitzgerald in Dublin, believes that blockchain-based tools are in the pipeline, but not yet to the degree that was predicted: "If you go back a number of years, there was a lot of talk that blockchain was just going to change the world, and I don't think it has," although she acknowledges that "things like virtual assets that are starting to really grow in popularity".

Despite all these developments, the principles of asset tracing remain the same, says Rees. "It is all about gathering evidence, building the case, demonstrating that money has moved in a particular way, [so that] you can make a claim on that asset." It is just the methods that are changing: "We are still using our investigative brains, it is like Robocop almost, we are controlling [the technology], but we are still the same inside."

In late 2019, the United Kingdom Jurisdiction Taskforce, part of the LawTech Delivery Panel, announced that crypto-assets can be treated as property. The announcement was heralded by **Sir Geoffrey Vos**, chancellor of the High Court of England and Wales as "a watershed for English law and the UK's jurisdictions".

"That might be regarded as some sort of English law land-grab, but at least we are trying to engage with the problem, it is not as if everybody else has," comments Oliver, on the basis that laying down guidance before an issue has arisen reverses the usual order of things for the better.

Across the continent, the European Union's Fifth Money Laundering Directive (5 MLD) has brought regulation to crypto-exchanges, crypto-to-fiat and fiat-to-crypto transactions with know your customer (KYC) checks. Meanwhile, the UK has gone even further, extending the obligations to all exchanges which deal with crypto-assets.

The introduction of 5 MLD is "a very significant moment" says Harty "because effectively it requires KYC in relation to certain virtual assets for the very first time". That raises a potential cultural change for cryptocurrencies: "Anonymity has always been an attraction for people who have been involved in virtual asset transactions." If there is less scope for anonymity, it should have an impact on the market.

As a result, 5 MLD "is definitely going to have an interesting effect on the desirability of virtual assets to those who are involved in nefarious activity. They might need to re-think", Harty adds.

Similar progress has been made in Ireland, which has had a couple of cases regarding the tracing and seizure of digital assets by the **Criminal Assets Bureau**, with the Irish courts "having no hesitation about saying 'clearly they are assets and capable of being recovered in this way'".

Pursuing those measures could lead to a thorny dilemma, and potential litigation, when a seizure deprives the asset holder of the ability to make trades, missing out on potential income.

As a result, she highlights the value of disclosure orders, which require the subject to reveal all of their assets. "As long as you draft it in a way that is broadly enough drafted to capture digital assets or digital wallets, encryption keys, you can at least identify the location of the assets and then you can take a view as to what you are going to do next."

Despite the changing technology, the legal principles must stay the same, argues Harty, calling for a focus on making them robust: "Generally the way to do that is to make your rules simpler rather than more complex. The more that you try to tailor things, specifically to deal with evolving technologies, the more likely you are that your rules are just going to be out of date very quickly with things that are evolving".

As for the UK, what impact Brexit will have on the authorities' ability to investigate and pursue digital assets remains to be seen. "One hopes that there will be similar enforcement mechanisms, exchange of information and the like, but only time will tell," concludes Oliver.

SAVE THE DATE

gli Global Legal Insights

BLOCKCHAIN REGULATION AND THE LAW 2020

28 APRIL
THE LAW SOCIETY, LONDON

Much has been discussed about the opportunities that blockchain technology presents. But what does the adoption of blockchain really mean to legal departments and is it as complex as it seems?

In the second of our annual blockchain-dedicated events, our expert panels will de-mystify blockchain technology and explore its practical implications to legal departments across a diverse range of industries with a focus on real-life case studies, while highlighting the risks, obligations, benefits and challenges associated with its implementation. In addition, the Symposium will examine the regulatory aspects of blockchain, with panels deliberating on how different jurisdictions are approaching the development and deployment of distributed ledger technologies.

MAJOR TOPICS TO INCLUDE:

- Smart contracts
- Trade, trade fi nance, payments, banking
- GDPR, IP, IT law
- eIDAS, supply chain management
- Security and fraud

CASE STUDY QUESTIONS UNDER DEBATE:

- What changes to legal departments will blockchain technology bring?
- What are the pros and cons of blockchain compared to traditional in-house legal procedures?
- Is distributed ledger technology secure and compliant with all regulations?
- What cost savings can blockchain technologies bring?

In association with the GLG publication **Global Legal Insights: Blockchain & Cryptocurrency Regulation**

For full details of sponsorship opportunities and ticket booking, contact our sales team at sales@glgroup.co.uk or on +44 207 367 0720.

FOLLOW @GLG_EVENTS FOR REGULAR UPDATES

glg EVENTS
global legal group
WWW.ICLG.COM/GLGEVENTS

Insolvency used as a tool in asset recovery

Andrew Stafford QC
Kobre & Kim

James Chapman-Booth
Kobre & Kim

Winning a favourable judgment or award is always a high for a litigation lawyer but, from the client's perspective, a judgment by itself is just a piece of paper. The client's objective is to receive money. For the client, it was never about the win, it was always about the money. Yet, collecting the money can be as hard-fought, as lengthy, and as costly a process as winning the award was in the first place.

This article addresses one of the specific tool-sets available to lawyers specialising in judgment enforcement – insolvency tools. It is important to note that the insolvency framework is a specialised tool: it is not a panacea, and so will not be suitable in every case. And, like any tool, it has greater utility in experienced hands than those of a novice. To understand how, when and where to deploy insolvency tools, it is important to take account of the alternative enforcement mechanisms, and to think about the need for recovery strategies generally.

No claimant should start litigation (or arbitration) assuming that the defendant, if defeated, will meekly pay up. Some – perhaps many – will do so. The defendant may be solvent and reputable, but even so the collection challenges might incentivise the defendant to hold out. Worse, there are some judgment debtors which are not reputable and which are of dubious solvency. For the disreputable judgment debtors, the judgment creditor's collection challenges align

with the judgment debtor's pre-disposition to hold out.

To make things more difficult for the claimant, the judgment enforcement landscape is becoming increasingly complex. Technological innovations such as electronic banking and faster payment schemes mean that assets can be acquired, transferred, and disposed of more easily than ever before. Consequently, judgment debtors are able to move their assets further afield, faster, with less effort and in ways that can be more difficult to track using conventional methods. With a click of a mouse, or even the tap of a smartphone screen, a delinquent judgment debtor can acquire a new shell company, convert their fiat currency to a readily transferrable cryptocurrency, or empty multiple bank accounts in mere seconds. New bank accounts, perhaps in a jurisdiction with aggressive confidentiality laws and limited frameworks for judgment recognition, might be opened without ever requiring the judgment debtor to physically step foot in the territory.

These types of collection challenges can make the lawyers' victory jig short-lived. Telling the clients that collection might take some time and will involve considerable further expense can quickly sour the client relationship. But the strain on the client relationship can be avoided by strategising about collection ahead of the judgment (speaking from experience, our firm sometimes finds itself called in to act as specialist co-counsel on enforcement more than a year before the judgment is delivered).

Of course, if a pre-judgment freezing order has already been granted by the court, the collection strategy has already been partly addressed – renew the freezing order so that it operates post-judgment, and close in on the assets identified and frozen. However, pre-judgment freezing orders are the exception rather than the rule. More often than not, the visible facts have not warranted the grant of a freezing order, yet the client nevertheless has a legitimate anxiety that the defendant will not pay without a further fight, or that, while the litigation was still pending, the defendant (now judgment debtor) will have taken steps to render itself more enforcement-proof.

A final and enforceable judgment will establish the defendant as a judgment debtor, and the claimant as an unsecured creditor. This principle underpins the use of the insolvency process as an asset recovery tool. An unpaid judgment debt forms the basis of a statutory demand; an unsatisfied statutory demand creates a presumption of insolvency which may then lead to a winding up or bankruptcy order.

Weighing up the insolvency option

When analysing the enforcement options, there are numerous issues to resolve in order to decide whether insolvency tools are the right fit. Only by working through these issues can a properly-informed decision about the suitability of insolvency be determined. Insolvency tools are powerful, but they can backfire badly if used incorrectly. In some cases, such strategies even if used properly may just be a bad fit. So, for example:

- Will there be competition for the debtor's assets? A winding-up order may leave the client at the wrong end of a queue of secured and unsecured creditors, rendering the immediate victory pyrrhic. An existential threat to the defendant may increase its determination to fight to the bitter end. Playing the strongman sounds good, but if the strongman is Samson you just end up pulling the temple onto your client's head.

Technological innovations such as electronic banking and faster payment schemes mean that assets can be acquired, transferred, and disposed of more easily than ever before

Playing the strongman sounds good, but if the strongman is Samson you just end up pulling the temple onto your client's head

- On the other hand, if available assets are limited, are there competing judgment creditors further down the collection road than your client? If so, it may be that insolvency will help to cancel that disadvantage to the client.
- Are any of the jurisdictions enforcement-friendly (or, indeed, unfriendly)? Some civil jurisdictions provide for pre-recognition attachment, which can make any insolvency strategies unnecessary. Alternatively, recognition in some jurisdictions can be so slow or hostile that the assets identified as being located within such a jurisdiction may be beyond the reach of a judgment creditor: it may be that the foreign court would instead be more receptive to an office-holder, like a liquidator, seeking recognition of the insolvency process.
- Is the target debtor asset-rich or revenue-rich? If analysis shows that that the target has strong regular revenue streams rather than piles of cash and property, insolvency would likely dam up those revenue streams. Maybe garnishment would collect the golden egg without killing the goose.
- To what will the debtor better respond? A consensual settlement of the outstanding judgment debt is always going to be quicker and cheaper for all parties concerned than an international war of attrition, but what will it take to get the debtor to want a consensual outcome? In some cases, commencing insolvency procedures may actually eliminate the option of driving the debtor to the settlement table. At the very least, insolvency brings into play an office-holder less vulnerable to commercial pressure points felt by the debtor, and more focused on the interests of creditors as a whole.
- Is the target based in only one jurisdiction or does it have assets, interests or affiliates in numerous jurisdictions? Although a multi-jurisdictional enforcement effort is naturally more complex, the international footprint of the debtor creates the opportunity to leverage differences in enforcement tools as between one jurisdiction and another. However, identifying the right lever requires not only experience and expertise in comparative law, but also a keen sense of timing and global control of the enforcement team. Timing is important because a step taken in one jurisdiction is likely to have knock-on effects elsewhere. Control is vital because a trigger-happy local co-counsel can disrupt the carefully developed global enforcement strategy.

Two points emerge from these typical issues. First, choosing to use insolvency tools should not be a reflex decision, but a sensible conclusion reached following a holistic analysis of the enforcement options. Second, accurate and comprehensive information about the target is vital – no informed decision can be made without information.

Leveraging cross-border discovery

Information is a vital commodity in the world of asset recovery. In any enforcement attempt, the judgment creditor must overcome an imbalance of knowledge: the judgment debtor will know where all of their assets are; the judgment creditor will not. Before the judgment creditor can enforce against an asset, they first need to know that it exists and, just as importantly, they must know where it resides. Information gathering therefore forms an important first step in any asset recovery campaign.

Some types of necessary information can be readily obtained through sources freely available to the public. Other information can be obtained through post-judgment discovery procedures.

To that end, a judgment creditor may apply for an order requiring the judgment debtor to attend court to provide information on oath about their means, or any other matter about which information is needed to enforce a judgment or order. If the order is granted, the judgment creditor can compel the judgment debtor to provide information about their assets worldwide.

In this context, once again there may be cross-border opportunities to leverage differences in discovery procedures. But there is the ever-present risk that using discovery procedures may simply tip-off the debtor, with the result that it re-doubles its efforts to render its assets enforcement-proof. Although claimants are sometimes motivated to seek disclosure of every document under the sun, this strategy is rarely sensible; rarer still is it accepted by the courts. And in some jurisdictions, third-party discovery may require the creditor to indemnify the third party for the costs of the discovery exercise – this can be a high price unless the discovery request is accurately made and is aimed at obtaining a narrow class of highly useful documents. Discovery requests in this context should be used as a scalpel, and not a sledgehammer.

The position of a liquidator seeking information may be very different. As an office-holder, a liquidator can obtain access to the internal documents held by the company. The liquidator may be able to summon the directors to answer questions, and (subject always to jurisdictional differences) may be able to seek post-judgment discovery on a wider and less costly basis. Since a liquidator wields the right to access documentation, proportionality is less of a concern – although economic and strategic factors should nevertheless help shape and narrow what is sought.

If the client believes that the defendant has been re-organising its affairs during the pendency of the litigation so as to render itself more enforcement-proof, this may tip the balance in favour of deploying insolvency tools. The liquidator has visibility into the internal affairs of the target entity, and the capacity to interrogate the directors can uncover activities designed to thwart enforcement efforts. Moreover, the liquidator can hold the directors and recipients to account and, where appropriate, can take recovery actions to restore to the company the assets which were placed elsewhere. Sometimes these powers are more valuable than the claimant's capacity to challenge transactions as being fraudulent transfers, useful though that power can be.

Akin to, but different from, liquidation is receivership. This places in the cross-hairs a specific revenue stream or asset. The receiver collects a specific asset and handles it in accordance with the distribution process sanction by the appointing court, leaving the debtor entity intact. Its availability varies from jurisdiction to jurisdiction. A court-appointed receiver is an office-holder and acts subject to the bespoke powers granted to him/her by the court. As with liquidation, an office-holder is accorded considerable respect by the courts. In the right case, receivership is the right insolvency tool.

Show me the money

But office-holders – whether liquidators or receivers – cost real money. The expense involved in deploying insolvency strategies demands an answer to the question – what are we going to do with all these powers? There is no useful purpose in triggering this strategy if the client's objective – getting money in its hands – is not going to be achieved, or at least significantly advanced, by these means.

Client buy-in is essential, and many clients – financially depleted by the litigation which led to the judgment and generally war-weary – may reasonably disagree with the idea of insolvency strategies that promise yet more expense. But a fully worked-out insolvency strategy might appeal to the client if the expense is to be met by a third party. The emergence of funders, willing in the right case to fund the cost of enforcement on a non-recourse basis in return for a share of the collections, can often render viable insolvency strategies which would be beyond the client's appetite for further expense. From the funder's perspective, the existence of a valid judgment or award removes several significant contingencies from its calculation of risk. From the client's perspective (and especially that of the General Counsel), it takes the expense and risk off the balance sheet – collections can become all up-side once acceptable commercial terms have been struck.

In our experience, there is no hard or fast rule about when, how, and where, to deploy an insolvency strategy in aid of judgment enforcement. But it should not be used without prior careful consideration. Whether or not the tool is appropriate will be determined by the specific facts of the case at hand: the location, type, and extent of assets; the extent of available information about those assets; the conduct and sophistication of the defendant; the client's litigation appetite; and wider commercial considerations are each factors that should be weighed before starting down the insolvency path. Nevertheless, when wielded properly, the insolvency framework can itself be an extremely valuable asset to the client.

Andrew Stafford QC is an English barrister and Queen's Counsel who represents corporations, hedge funds and high-net-worth individuals in complex, high-value litigations spanning multiple jurisdictions and that involve significant cross-border elements. He has particular experience in international judgment enforcement, developing and executing strategies designed to secure effective collection of awards and judgments, including relating to enforcement against sovereign judgment debtors. In the area of financial services and products, Andrew handles swaps litigation, including matters of currency fixing related to Libor, Euribor and foreign exchange markets.

Andrew also represents clients in joint venture and partnership disputes, as well as in regulatory defence matters involving UK authorities.

A highly regarded appellate advocate and trial lawyer, Andrew appears in the Supreme Court of the United Kingdom and acts in international arbitrations on a range of matters, including financial derivatives, insurance and international commercial fraud. He has been cited by industry publications as "a really good lateral thinker" and "a great tactician" with "fantastic courtroom demeanor".

andrew.stafford@kobrekim.com

James Chapman-Booth is an English barrister who focuses on cross-border commercial litigation. His experience includes disputes related to financial products and services, insolvency proceedings and U.S. regulatory enforcement matters.

James studied English law and was called to the Bar at the Honourable Society of the Middle Temple.

james.booth@kobrekim.com

Kobre & Kim is an Am Law 200 global law firm focused exclusively on disputes and investigations, often involving fraud and misconduct. Recognised as the premier firm for cross-border disputes, the firm has a particular focus on financial products and services litigation, insolvency disputes, intellectual property litigation, international judgment enforcement and asset recovery, and U.S. government enforcement and regulatory investigations. By avoiding repeat client relationships, and the conflicts of interests that come with them, the firm maintains its independence as advocates ready to litigate against virtually any institution.

The firm has more than 150 lawyers and analysts located in multiple jurisdictions throughout its 14 locations around the world.

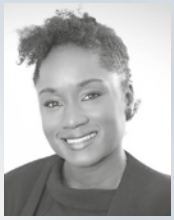
www.kobrekim.com

KOBRE & KIM

International criminal law tools in aid of civil asset recovery

Alun Jones QC
Great James Street Chambers

Nick Beechey
Great James Street Chambers



Samantha Davies
Great James Street Chambers

In our experience, lawyers and accountants take insufficient account of the value of criminal procedure tools in international asset recovery. These are more far-reaching and draconian than conventional tools for recovery in the civil courts, but they require the co-operation of law enforcement public authorities. They are important weapons in the arsenal of any practitioner involved in asset recovery.

This article considers both incoming requests for recovery of assets allegedly the proceeds of crime and, to the extent that other states and territories reflect our own provisions, requests to other territories.

Norwich Pharmacal

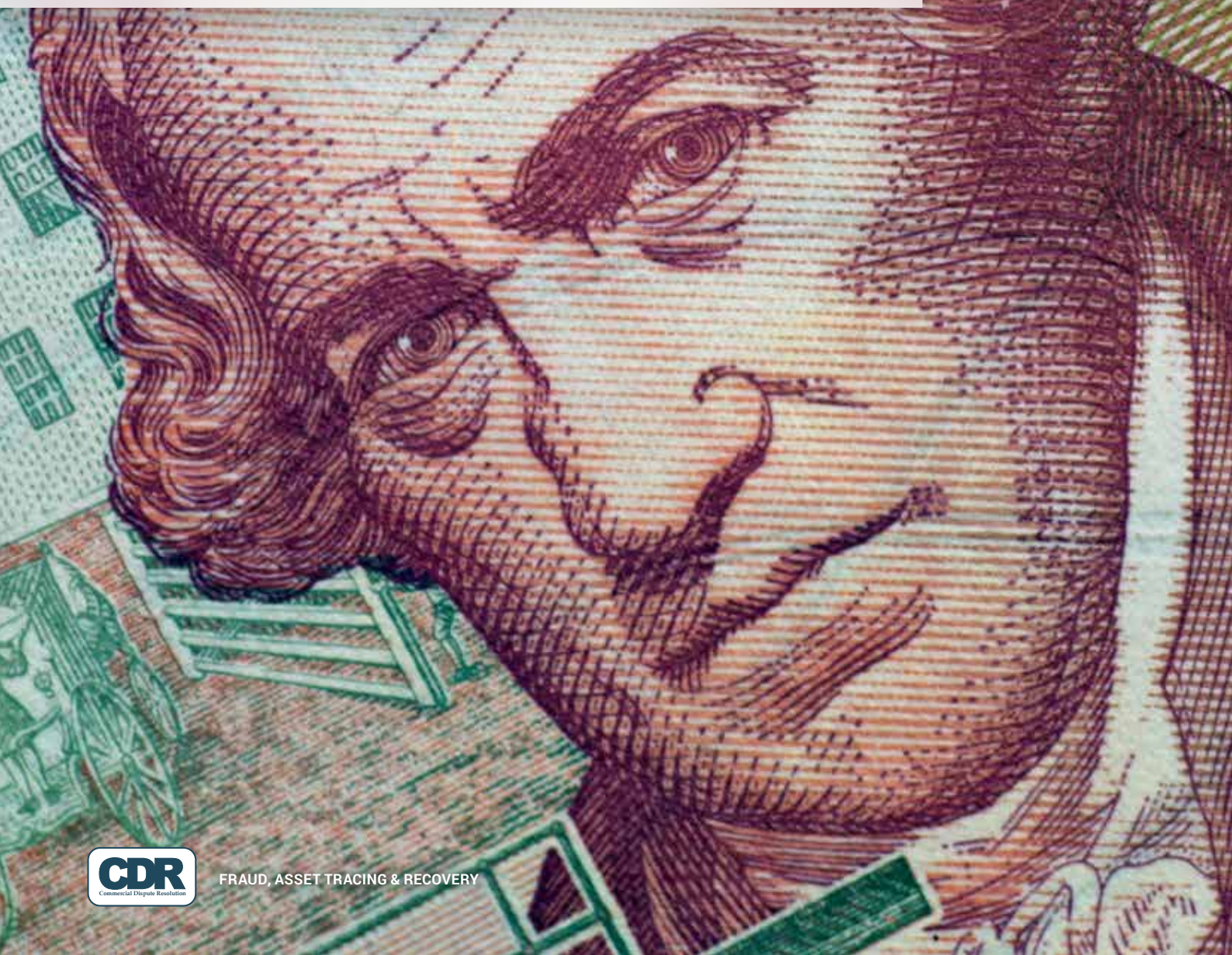
The key tool of the civil litigator is Norwich Pharmacal relief. This is available to a party who can show a good arguable case of wrongdoing and/or the existence of a right which has been infringed. Evidence of sufficient involvement of the respondent will be required and the applicant will need to show that Norwich Pharmacal relief is necessary, as this has a strong impact on the

exercise of the court's discretion.

Recent case law has called into question the availability of relief where the substantive proceedings are to take place overseas. Relief has previously been granted against English respondents in respect of proceedings due to take place in Italy, France and Spain, among other jurisdictions. The reason for this more recent curtailment of the Norwich Pharmacal jurisdiction is the court's view that Parliament could not have intended that this common law remedy should survive the introduction of a clear statutory regime. *R (on the application of Omar and Others) v Secretary of State for Foreign and Commonwealth Affairs* [2013] EWCA 118 declares that Norwich Pharmacal relief cannot be obtained in this jurisdiction for use in foreign criminal proceedings. The decision upholds the distinction between the criminal and civil jurisdictions. As discussed in the judgment of *Omar and Others*, clear safeguards are applicable in the mutual legal assistance regimes which have created clear processes for obtaining evidence for use in overseas criminal proceedings. These very same principles have nonetheless also been applied in the context of applications for Norwich Pharmacal relief in respect of prospective civil litigation overseas.

Where a party wishes to obtain evidence in this jurisdiction for use in civil proceedings overseas, that party must employ the processes available under the statutory regime, i.e. Evidence (Proceedings in Other Jurisdictions) Act 1975 (the "1975 Act"). Stringent tests are applicable to the obtaining of evidence in respect of each of these mechanisms. Commonwealth case law suggests that the relief may be available where the applicant seeks to obtain information as opposed to evidence; see *Secilpar v Fiduciary Trust Limited* [2003-04] Gib LR 463, Court of Appeal, a decision of the Gibraltar Court of Appeal. These challenges do not arise where the Norwich Pharmacal relief is sought in respect of proceedings in this jurisdiction.

By way of contrast, we have sought to examine those criminal law tools which may assist parties engaged in asset recovery proceedings.



International schemes

Mutual legal assistance in criminal matters has been available for decades, in the Council of Europe Convention of Mutual Legal Assistance of 1959, the Commonwealth Harare scheme (latest version 2011) and the bilateral and multilateral instruments listed on the Home Office website. Their provisions are not considered in detail here, because in the UK the governing statute, the Crime International Co-operation Act 2003 ("CICA"), makes provision for the making and receipt of legal assistance requests to any territory in the world, whether or not a territory is party to a Convention or arrangement, but subject to the general discretion to refuse them. In this way, mutual legal assistance in criminal matters differs importantly from extradition arrangements, which generally insist on reciprocity of provision.

The UK requires all requests for obtaining evidence located within the jurisdiction to be transmitted through the central authority. The Home Secretary is responsible for mutual assistance in criminal matters in England, Wales and Northern Ireland. Her functions are presently exercised by the Home Office's Judicial Cooperation Unit which acts as the UK Central Authority. All requests for evidence located within the UK must be processed through the central authority. Notably, this process of indirect transmission does not apply to requests for evidence abroad from the UK Central Authority who may make such requests directly to a foreign judicial authority. The process can be long and arduous but works effectively. In 2018, the UK Central Authority received 6,649 incoming requests for Mutual Legal Assistance. A significant proportion of these were made through the European Investigation Order (2,874 in total).

The approach and policy of the Home Office, the "Central Authority" to the operation of this Act, is set out in its mutual legal assistance guidelines. It is important to appreciate that overseas authorities may approach people in this country, including police forces, to seek their voluntary assistance, where recourse to formal legal machinery is unnecessary.

In making requests to other jurisdictions, the provisions of the relevant international instruments must be consulted. Almost all European states are party to the 1959 Convention; and all UK dependent territories and Commonwealth countries to the Harare Convention. The Harare scheme contains many provisions which mirror the European Convention of 1959 but provides wider grounds for refusal of a request for assistance, for example: in the absence of dual criminality; where there was a political offence; and where the principle of double jeopardy might be infringed. In some ways the EU schemes have followed some of the lessons of the Harare Scheme because it included mechanisms for tracing, confiscation and seizing of assets before these were adopted in the EU context. Although mechanisms for mutual legal assistance exist and are supported by the Commonwealth Secretariat, there have been cases where the courts have dispensed with these provisions and in some cases travelled to the relevant territory to hear the evidence directly, *Attorney-General of Zambia v Meer Care & Desai (A Firm)* [2007] EWHC 952 is a case in point. Courts are not always restricted by these very formal provisions.

Under CICA, evidence obtained from foreign states pursuant to letters of request may not be used for any purpose other than that specified in the request without the consent of the requested territory, *Crown Prosecution Service v Gohil* [2013] 2 W.L.R. 1123. However, although a person may not adduce documents obtained through mutual legal assistance in other proceedings without the consent of the requested state, such an individual may use the documents as a basis for conducting their own investigations if consent cannot be obtained. This restriction on the use of documents obtained through mutual legal assistance is therefore not as onerous as it might first appear.

Those advising on the recovery of assets removed from other territories should be aware that all these third countries will have "central authorities" whose assistance can be invoked where there are reasonable grounds for believing that offences have been committed. Letters of Request can be made simply, often with the minimum of evidence and a simple narrative of (i) the criminal conduct alleged, and (ii) information as to where it is believed the assets have been placed. In most cases, the procedure permits the central authority of the requested party to invoke its domestic criminal enforcement procedures in aid of the requesting party.

The recovery of criminally obtained assets is likely to be easier if the offender is simultaneously arrested for extradition in the requesting country. Extradition is outside the scope of this article, but the joint use of extradition and asset recovery procedures is likely to concentrate minds, and to produce quicker results than the simple use of civil procedures for recovery. We have come across

many cases in which lawyers and accountants seeking the recovery of assets fail to consider the use of extradition procedures.

UK mutual legal assistance statutory provisions

The following provisions of CICA applying to incoming requests for legal assistance are likely to be duplicated in European or Commonwealth jurisdictions and the USA.

Sections 12–28 deal with requests to the Central Authority made by overseas prosecutors or criminal courts. If such a request is made, the Central Authority may nominate a court where evidence can be obtained either orally or in documentary form, by using the domestic witness summons, production order procedures (POCA, PACE, etc.) or taking evidence on oath (section 15). If the case appears to involve serious or complex fraud, it may be referred to the Serious Fraud Office, which can use its familiar powers under the Criminal Justice Act 1987. The Central Authority may direct that a search warrant be applied for under section 16, which permits the powers of Part 2 of PACE to be invoked. These provide for warrants to be obtained either from a justice of the peace or, in the case of "special procedure material" (essentially, business confidential documents, bank accountancy records, etc.), from a Circuit Judge.

Not all international cooperation in criminal matters requires the involvement of the UK Central Authority and/or the very formal process of Letters of Request. A great deal of the UK's efforts in international cooperation in criminal matters is dealt with by the NCA. The NCA acts as the UK Central Bureau for Interpol. The NCA manages the routine exchange of police and law enforcement information in matters of serious and organised crime. The NCA has wide-ranging powers in respect of its international cooperation capability. The NCA may interview witnesses or suspects in criminal investigations in this jurisdiction on behalf of overseas authorities where such persons are willing to cooperate. The NCA may share information and intelligence concerning investigations into offences which have been committed in the UK. Although such information may not be used in proceedings, it represents significant assistance in information gathering. The NCA may also assist a foreign law enforcement agency with asset tracing enquiries, provide details of an individual's medical or dental records (where consent has been given) and furnish information from publicly available sources. The range of assistance available through the NCA circumvents the formal and often arduous approach required by Letters of Request.

European Investigation Orders

The European Investigation Order (EIO) has radically changed the process for cooperation between EU territories. The Criminal Justice (European Investigation Order) Regulations 2017 (SI 2017/730) came into force on 31 July 2017 and give effect to the EIO Directive. An EIO can be used to obtain evidence that already exists and is directly available in the form of items, documents or data. An EIO may also be used for the purpose of gathering evidence and may request the use of investigative measures including telephone interceptions, covert investigation and banking information.

An EIO is issued in a standard form and then translated into the official language of the executing state. It provides clearer timeframes for securing evidence as it must be recognised and acted upon within a fixed deadline of 30 days maximum (for evidence which already exists) and 120 days (for investigative measures which need to be carried out). The execution of an EIO is not subject to a requirement of dual criminality if the offence under investigation is punishable by a custodial sentence of at least three years and is included on the list of offences set out in the EIO Directive.

A constable acting with the consent of a prosecuting authority may apply for an EIO. An application for an EIO may also be made by a prosecuting authority and any party to a prosecution, including the defendant. The EIO represents a sea change in mutual legal assistance between European territories. The mechanism that will replace it once the Law Enforcement and Security (Amendment) (EU Exit) Regulations 2019 come into force remains to be seen.

Warrants and notices to produce/ productions orders

These powers may also be used to apply for notices to produce, as defined and provided for in

Schedule 1, paragraph 2, of PACE for confidential business or other financial information, from banks, accountants, etc., of production orders under section 345 and following of POCA; and notices to produce within sections 2 and 3 of the Criminal Justice Act 1987 on the application of the SFO. None of these powers may be used to obtain legally privileged material. It is rare for the use of these powers to be challenged by judicial review, partly because financial institutions often consider, rightly, that to inform their customers of the application for such an order will amount to "tipping-off"; but also, partly because they are persuaded, wrongly, not to inform customers where the suspects are already aware of the inquiry. An example of the successful review of a production order is *R (Chatwani) v NCA (No 2)* [2015] EWHC 1284 (Admin).

The provisions of section 16(2)(b) of PACE should be noted. This permits a constable who is a member of a joint investigation team, as defined by section 16(5), to apply for a PACE warrant without reference from the Central Authority. Under section 16 and Schedule 1 of PACE, a justice of the peace or judge can authorise persons to accompany a searching constable, and also, under supervision of such constable, to seize material himself. It is therefore possible for such material to be seized by overseas officials and removed from the UK under section 19 CICA before any challenge for judicial review can be made; whereas sections 21 and 22 of PACE provide for the retention of such material in England and Wales and allow for inspection by an interested person. These are startlingly intrusive powers.

There is developed jurisprudence on the legality of search warrants. Clear adherence to the statutory preconditions of section 2 or Schedule 1, paragraphs 2 and 3 of PACE is required. Material to be seized must be identified with particularity. Legally privileged material may not be seized (PACE, section 19). Various protections are enshrined for the benefit of occupiers of premises.

Above all, a duty of candour is imposed, so that the applicant for a search warrant must disclose to the justice or judge anything which he knows the occupier of premises would say in opposition to the grant of the warrants if he were present; see, generally, *R (Rawlinson and Hunter) v Central Criminal Court and others* [2012] EHHC 2254. This principle applies also to the obtaining of production orders and notices to produce.

In our experience, applications for search warrants and production orders frequently fail to observe this principle, and it is difficult for police

officers applying for warrants based on overseas requests to be able to satisfy a judge that all relevant information has been disclosed. The consequences may be grave, especially where section 19 of PACE permits the removal from the jurisdiction of seized material quickly and simply.

Judicial review is available to challenge the legality and rationality of search warrants.

The scheme of Proceeds of Crime Act 2002 (POCA); restraint and confiscation orders

Before its amendment by the Criminal Finances Act 2017 ("CFA"), POCA had four distinct means of confiscating the proceeds of crime: confiscation following criminal conviction (Part 2); civil recovery in the absence of conviction (Part 5); cash forfeiture, where there are reasonable grounds to suspect that cash is the proceeds of crime (Part 5); and criminal taxation, which allows the NCA to access revenue powers to tax income where there are reasonable grounds to suspect it is the proceeds of crime (Part 6). Part 2 confiscation remains the main tool for criminal proceeds asset recovery in the UK.

The POCA provisions apply equally to prosecutions brought by way of private prosecution. Private prosecution as a tool for asset recovery can hold attractions, including the award of costs from central funds even if the prosecution does not succeed, and has grown in use in recent times, in part as a consequence of a near 30% fall in the prosecution by the state of commercial crime. An advantage of this means of asset recovery is that the confiscation is not directed towards any particular asset and does not deprive the defendant or any other person of title to any property; that the criminal lifestyle provisions, where they apply, bite more widely than benefit derived from the index offence; and that there are significant enforcement sanctions in the form of terms of imprisonment in default, once an order is made. Compensation can be ordered to be paid from confiscation.

Under section 74 POCA, where a confiscation order has been made and it is believed that realisable property may be held outside the UK, a request may be made to the Secretary of State to forward to the relevant government to secure that any person is prohibited from dealing with the realisable property, that it is realised, and the proceeds applied in accordance with the law in that country.

Restraint under POCA can be applied for by a prosecuting authority or those with authorised arrangements with a prosecuting authority. It can be applied for pre-charge, so long as the defendant is to be charged. There is a requirement that a criminal investigation or prosecution in England and Wales has started and that there are reasonable grounds to suspect that the offender has benefited from his criminal conduct. A person can be restrained from dealing with any realisable property, whether or not described in the order and whether or not transferred after the order is made. There is no bar on hearsay evidence in proceedings for restraint.

Once a restraint order is made, the court may make an order requiring the defendant to disclose, by affidavit, the nature and whereabouts of his assets, wherever they may be in the world. In relation to confiscation investigations a disclosure order can require a person to answer questions, provide information and disclose documents.

If a restraint order is made, the court can order the relocation of assets that are outside England and Wales to be brought within the jurisdiction and can appoint a receiver, either pre-conviction to manage the assets or post-conviction to satisfy the order.

Customer Information Orders and Account Monitoring Orders may be made where the court is satisfied that the person specified in the order is subject to a confiscation or money laundering investigation, the order is for the purposes of investigation and is sought against a financial institution specified in the application.

The Criminal Finance Act 2017

The CFA made a number of amendments to POCA.

The CFA introduced Unexplained Wealth Orders (UWOs) and Interim Freezing Orders (IFOs), which came into force on 31 January 2018. The NCA obtained the first two orders a month later. These provisions extend the ambit of POCA, which until their introduction required prosecutors to show at least a good arguable case that assets represent the proceeds of crime or are owned by someone who has benefited from crime before they could be frozen.

An application for a UWO can be made *ex parte*

and in private. IFOs, if sought, must be sought at the same time as a UWO. The result of an application is therefore that the legal owner may be unable to sell or transfer any assets until the matter has been concluded.

The court has to be satisfied of a number of factors: that there is reasonable cause to believe that the respondent holds the property, and its value is greater than £50,000; that there are reasonable grounds to suspect that the known sources of the respondent's lawfully obtained income would have been insufficient for the purposes of enabling the respondent to obtain the property; and that the holder of property is either a Politically Exposed Person (PEP) or that there are reasonable grounds for suspecting that the holder, or a person connected with them, is or has been involved in serious crime. A PEP is an individual who has been entrusted with prominent public functions by an international organisation or state, other than the UK or an EEA state, or a family member or close associate of such a person. PEPs can include, for example, government ministers, MPs or equivalent, and senior judiciary. Close associates can include those who own property with or for a PEP, or have a close business relationship with a PEP. It is immaterial that the property may be jointly held by another person. Once so satisfied the court will, if applied for, invariably impose an IFO at this stage.

If this relatively low threshold is met, the burden moves to the respondent, who has to serve a statement in response showing the legitimacy of the funds used to acquire the property subject to the order. If no statement in response is forthcoming, the property is presumed recoverable under Part 5. If there is a statement in response, the applicant has 60 days to decide whether to take further enforcement or investigatory action.

If an UWO is made in respect of any property, the enforcement authority may send a request for assistance to the Secretary of State with a view to the request being forwarded to a foreign government to secure that any person is prohibited from dealing with the property in their state and/or for assistance with the management of the property, including securing its detention, custody or preservation.

It is a criminal offence, in a response, to knowingly or recklessly make a false or misleading statement in relation to a material particular. The offence is punishable with up to two years' imprisonment and/or a fine. A statement made in response may not be used in criminal proceedings against the respondent.

The far-reaching effect of UWOs comes from the fact that investigators do not have to show a suspicion that the property represents the proceeds of crime or that the holder has in fact committed any offence, and that the burden of proof is reversed.

The recent case of Malik Riaz Hussain (reported in the media on 4 December 2019), whose UK bank accounts were frozen by the NCA using the CFA 2017 provisions and who entered a voluntary agreement to surrender £140 million held in nine accounts along with a further £50 million London property, shows on the one hand the force of these provisions and at the same time that the NCA will negotiate a settlement.

The CFA also introduced bank account freezing orders and forfeiture orders (AFOs), forfeiture of listed assets and corporate offences of failure to prevent facilitation of tax evasion, as well as expanding civil recovery powers by introducing disclosure orders applicable to those carrying on a business in the regulated sector.

AFOs largely mirror the POCA provisions relating to cash forfeiture but, as the name suggests, are applicable to funds held in bank accounts. An enforcement officer applies for a freezing order if he has reasonable grounds to suspect that money (minimum amount £1,000) held in an account with a bank or building society is recoverable property or is intended by any person for use in unlawful conduct. The application may relate to all or part of the credit in the account. The order is granted if the court finds there are reasonable grounds to suspect, as above. An account forfeiture application is made once a freezing order is in place. A senior officer must apply for forfeiture on notice, which will be ordered if the court is satisfied that the money is recoverable property and is intended by any person for use in unlawful conduct. A respondent has 30 days to object.

CFA 2017 introduced provisions for the search, seizure and detention of listed assets, the definition of which is precious metals and stones, watches, works of art, face-value vouchers and postage stamps. The test for forfeiture of listed assets is the same as for money in bank accounts.

External Confiscation Orders

The EU Framework Decision 2003/577/JHA and Framework Decision 2006/783/JHA respectively provide for the execution of orders freezing property and the application of mutual recognition of confiscation orders in the EU. The UK implemented these Decisions in The Criminal Justice and Data Protection (Protocol No 36) Regulation 2014.

Under these Decisions, a Member state can send restraint orders or confiscation orders to another Member state where the subject of the order lives or has property or income in the receiving state. The receiving state directly implements the order under its own national rules.

Regulations 6 and 7 govern the certification and sending of domestic restraint orders overseas and Regulations 11 and 12 likewise govern domestic confiscation orders.

Regulation 8 states that when a UK prosecuting authority receives an overseas restraint order and three conditions are satisfied, the prosecutor must send a copy of the order to the Crown Court for execution. The order must relate to criminal proceedings instituted in the Member state or a criminal investigation being carried on there, and prohibits dealing with property which is in England and Wales and which the appropriate court or authority considers has been or is likely to be used for the purposes of criminal conduct, or is the proceeds of criminal conduct. The three conditions that have to be satisfied are that: A) the criminal conduct is not an act of terrorism or for the purposes of terrorism; B) the order is accompanied by a certificate which gives the specified information, is signed by or on behalf of the court or authority which made the order, includes a statement as to the accuracy of the information given in it and, if not in English, is translated; and C) is accompanied by another order for confiscation made by a court exercising criminal jurisdiction in the Member state, or an indication that such an order is likely to be made and when it is expected to be sent.

Regulation 9 states that where the Crown Court receives an overseas restraint order it must consider giving effect to the order no later than the end of the next working day. In exceptional circumstances it may delay, but for no longer than the end of the fifth working day. A hearing may be held which must be private, and to give effect to the order the prosecutor must be present or have had an opportunity to make representations. The court may decide not to give effect to the order if to do so would be impossible as a consequence of immunity under English law, or it would be incompatible with Convention rights.

Regulation 13 relates to overseas confiscation orders. An overseas order is one made by an appropriate court or authority in a Member

state for the confiscation of property which is in England and Wales, or is the property of a person (or body of persons whether corporate or not) normally resident in England and Wales, and which the appropriate court or authority considers was used or intended for use for the purposes of criminal conduct, or is the proceeds of criminal conduct. Three conditions must be met: A) that a person has been convicted of that criminal conduct in the Member state; B) that the order was made at the conclusion of the proceedings that gave rise to the conviction; and C) that the order is accompanied by a certificate that gives the specified information, is signed by or on behalf of the court or authority which made the order, if not in English is translated and includes a statement of accuracy as to the information given. Criminal conduct is that listed in Article 6 of the 2006 Decision or that which would constitute a criminal offence in the UK if it occurred there.

On receiving an overseas confiscation order, the Crown Court must consider giving effect to it. Regulation 14 sets out the criteria for giving effect to the order. There are only three grounds of challenge to the giving effect to an order: if it would be statute barred; impossible to give effect to the order as a consequence of immunity; or that to give effect to the order would be incompatible with any Convention rights (Regulation 14(4)).

Substantive challenges to these EU orders are as hemmed in with difficulty as is the case with challenges to EAWs. The executing court cannot consider a substantive challenge to the making of the order; those arguments are for the courts of the issuing state (*A v DPP* [2016] EWCA Crim 1393).

Non-EU

The recognition and enforcement of non-EU confiscation orders is based in general MLA procedure. Any non-EU jurisdiction may make an MLA request to restrain or recover the proceeds of crime located within the UK. Requests require dual criminality and come via Letters of Request.

The Proceeds of Crime Act 2002 (External Requests and Orders) Order 2005 governs requests for restraint and confiscation. Requests should be made to the UK Central Authority.

For restraint, the request should show that an order has been made in the requesting jurisdiction; confirm that there is dual criminality; detail the ongoing criminal investigation into acquisitive crime or money laundering in the requesting state; set out the material facts, including any defence advanced; state why there is reasonable cause to believe the subject named in the request has benefited from his criminal conduct and why there are reasonable grounds to believe that the property may be needed to satisfy the external order; set out why the order is necessary; give details of the subject's name, address, date and place of birth and present location; detail the property in the UK to be restrained, the person holding it and the nexus between the subject and the property; state whether prior assistance has been provided; detail any other court orders made in the requesting state against the subject; detail all known property outside the UK and state why property in the UK must be restrained because there are insufficient assets elsewhere; and state whether the requesting state objects to the UK courts allowing access to restrained funds for the purposes of living and legal expenses.

Requests relating to a confiscation order should follow a similar form. It must be confirmed in the request that: there is dual criminality; the person named in the order is convicted and no appeal is outstanding; the order is in force and not subject to appeal; all or a certain amount of the order remains unpaid in the requesting state or other property there remains unrecovered; the order has the purpose of recovering property or the value of property received in connection with the crime; the order can be enforced outside the jurisdiction of the requesting state; the material facts of the case, including any defence advanced; why the order is necessary; personal details; detail of the property to be confiscated held in the UK; prior assistance; other court orders; details of all known property held outside the UK; and the original or authenticated copy of the original order.

In relation to restraint, the Crown Court retains a permissive discretion as the Regulation states the court *may* make an order; in relation to confiscation, if all the criteria are satisfied the court *must* make the order.

The court will give effect to the confiscation order request if: the external order was made consequent to the conviction of the person named in the order and no appeal is outstanding; the external order is in force and no appeal is outstanding; giving effect to the order would not be incompatible with any Convention rights; and the external order authorises the confiscation of property specified, other than money that it is not subject to a charge under any of the provisions in Article 21(6) of the 2005 Order.

Once again, substantive challenges to the order cannot be raised in the executing court. In seeking to challenge an order, one has to look

at whether the appropriate authority issued the MLA request; whether permission was obtained to use the information contained in the letter of request; whether any appeals are extant; whether any Convention challenges arise on the facts; and whether anything on the face of the request leads to questions as to its soundness.

EU Joint Investigation Teams (JITs)

JITs are provided for by Article 13 of the EU Mutual Legal Assistance Convention and the Framework Decision 2002/465/JHA. Their statutory recognition appears in sections 16 and 17 of CICA and Article 9 of the *Crime International Co-operation Act 20003 Exercise of Functions Order 2013*. See generally *R (Superior Import and Export Ltd) v HMRC* [2017] EWHC 3172.

A JIT is an international cooperation tool based on a legal agreement between two or more EU Member states to undertake joint cross-border criminal investigations during a fixed period of time, including the intensive and direct exchange of information between its members, and can be set up to include competent authorities in non-Member states. JITs are set up for difficult and demanding cross-border investigations and investigations into criminal offences in which the circumstances of the case necessitate coordinated, concerted action in the Member states involved.

JITs' main purpose is to facilitate the coordination of investigations and prosecutions, allowing for the direct gathering and exchange of information and evidence without the need to use the usual channels of MLA. Information and evidence gathered can be shared on the sole basis of the JIT agreement. They are therefore symptomatic of the general move away from legal framework MLA.

The purpose, composition and duration of the JIT is set out in the agreement. A single JIT can deal with investigations into more than one type of crime. Investigations do not have to be ongoing in both or all states involved. Information and evidence is limited by the specialty rule; it can only be used for the purpose for which the JIT was set up. However, parties to the JIT can amend the agreement by mutual consent, to include extending the use to which information obtained can be put.

The agreement specifies JIT leaders (who have a supervisory role) and members (law enforcement authorities). Members can include officials of bodies other than the law enforcement agencies of participating states, for instance officers of Europol. All members can be present and tasked to carry out investigative measures and can share information available in their own state. When acting as part of a JIT, members are bound by the law of the state in which they are acting. National legislation in the state in which proceedings are instituted regulates the admissibility and disclosure of evidence and information obtained under a JIT. It can be difficult to obtain disclosure of the JIT agreement itself, but this was achieved in *The Queen (on the application of) Superior Import/Export Limited, Johal, Johal and the Commissioners for HMRC, Birmingham Magistrates' Court* [2017] EWHC 3172 (Admin).

A JIT can include agreement on consultation over the timing, method of intervention and best manner in which to undertake eventual legal proceedings, and may leave open the possibility of prosecution and confiscation proceedings being instituted in any of the states involved, depending on the outcome of investigations.

JITs can be supported by Eurojust. This extends to financial and logistical support, expertise and judicial analysis. In 2018, Eurojust supported 235 JITs, of which 150 were ongoing and 85 newly signed. Forty-seven of those 85 newly signed concerned money laundering, fraud, crimes against EU financial interests, corruption and cybercrime, with terrorism, drug and people smuggling comprising the bulk of the remainder (*Eurojust Annual Report 2018*).

Conclusion

There exists a formidable array of powers available for mutual legal assistance where there are reasonable grounds to believe, or sometimes, reasonable grounds to suspect, that a profit or benefit has been made by criminal conduct. However, the statutory requirements, even where comparatively simple, must be properly observed. They are open to effective legal challenge in the case of over-zealous use.

Note

This article reflects the applicable law at the time of writing. The coming into force of the Law Enforcement and Security (Amendment) (EU Exit) Regulations 2019 will likely impact upon the provisions relating to EU law. In the future, consideration will need to be given to the impact and effect of the processes which replace these provisions following EU Exit Day.

Alun Jones QC has, for many years, specialised in international crime, extradition, asset recovery, and mutual legal assistance. He has conducted, as leading counsel, over 35 cases in the House of Lords, Supreme Court or Privy Council in these areas, and dozens of similar cases in other appellate or review courts, in the UK and abroad. He represents governments, companies and private individuals. Alun regularly writes, lectures and broadcasts in these subjects and has, in recent years, developed a specialisation in data protection and computer misuse. He has been Head of Great James Street Chambers, which he founded, for 15 years. He currently advises extensively in the UK, Asia, the Middle East and Africa on asset recovery and the use of mutual legal assistance. He is Chairman and non-executive director of Testenium Limited, a UK company set up to develop software to secure governmental and commercial data from unlawful access.

alun.jones@greatjames.co.uk

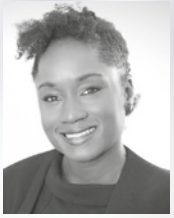
Nick Beechey is a leading junior whose practice is primarily defending clients in business and financial services crime as well as appearing in serious criminal trials. He has an extensive Appellate Court practice.

Nick is regularly instructed defending high-value, large-scale fraud and similar cases where there is a substantial amount of evidence and technical detail.

Nick regularly works within sizeable legal teams such as professional clients, relevant experts and junior counsel, recognising the benefit of giving advice at an early stage. The advice he provides is always clear and straightforward, in order to help achieve the best results for his lay clients.

Nick has a strong practice in advising on appeals against conviction and sentence where he was not the original advocate, providing clear and cogent written advice and grounds of appeal. These referrals have resulted in him appearing in the Court of Appeal on a regular basis.

nick.beechey@greatjames.co.uk



Samantha Davies is an experienced barrister who combines her expertise in white-collar crime with commercial litigation, extradition and international arbitration. As a specialist white-collar crime practitioner, she has acted for both prosecuting agencies and companies in this jurisdiction and overseas.

Samantha spent over two years advising a French multinational on its anti-bribery and anti-corruption polices including the review of contractual arrangements and payment processes within the business units to ensure that they were compliant with the Bribery Act 2010.

Samantha has advised both companies and governments in Africa upon various aspects of English law. She has advised extensively upon commercial disputes as well as anti-corruption and human rights obligations for both governments and corporations.

Samantha also continues to work with NGOs on anti-corruption and human rights initiatives across Africa and the United Kingdom. She speaks French and Spanish fluently and often travels and works abroad, as required by the relevant project.

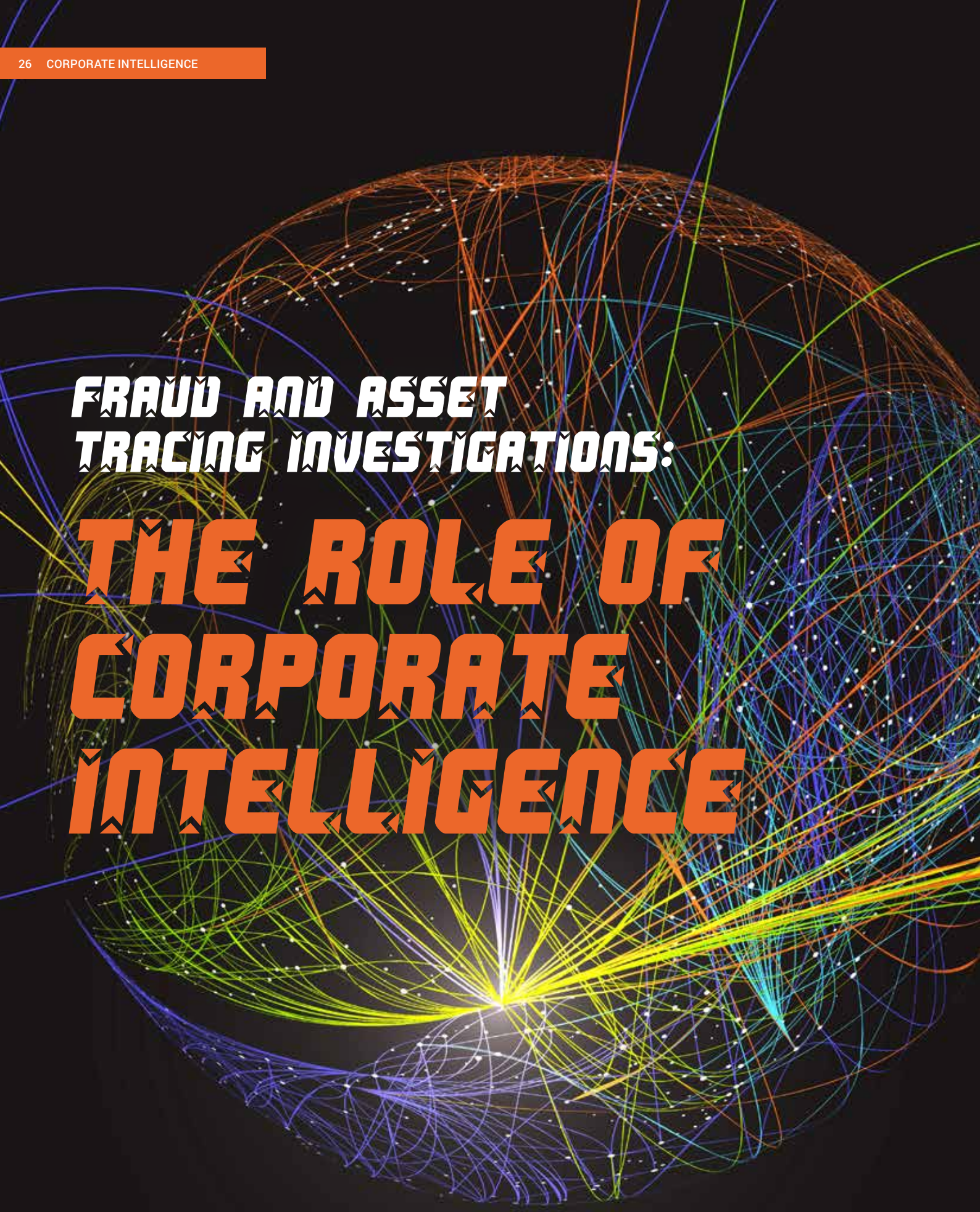
samantha.davies@greatjames.co.uk

Great James Street Chambers' reputation for excellence at the Bar is founded on the strength, at all levels, of its individual members. Great James Street Chambers has swiftly become prominent in a crowded market, successfully establishing itself as a leader in niche areas of law such as financial and general crime, extradition, search warrants, mutual legal assistance, commercial litigation, civil fraud, arbitration and mediation.

We have numerous members of Chambers who are dual qualified. In addition to being called to the UK Bar, we have members called to the Bar in Sierra Leone, Nigeria, Cameroon, Hong Kong, Republic of Ireland, Australia and St Vincent & Grenada. Our members advise on corporate offending, financial regulation, bribery and corruption, instructed by national and international law firms representing individuals and multinational companies.

www.greatjames.co.uk

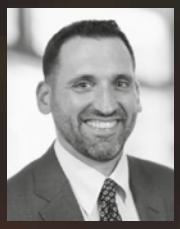
Great James Street



FRAUD AND ASSET TRACING INVESTIGATIONS:

THE ROLE OF CORPORATE INTELLIGENCE

Alexander Davies
BDO



Peter Woglom
BDO

Setting the Scene

The aim of this article is to give a sense of the range of investigative possibilities offered by corporate intelligence work, focusing particularly on fraud and asset tracing investigations.

Of course, fraud investigations and asset tracing investigations are very different beasts. The typical circumstances in which a fraud investigation is required are very different from those forming the background to an asset tracing investigation (even if there are situations where the latter can flow from the former), and the specific objectives and areas of focus are also quite different between the two. Nonetheless, a good number of the tools available to corporate intelligence investigators can usefully be applied to both types of investigation so – as with this book as a whole – this chapter will encompass both.

A further observation should be made before we proceed further: both 'fraud' and 'asset tracing' are widely used as shorthand terms for a wide array of investigations. As investigators, we often refer to investigations of 'fraud or other malfeasance' to encompass investigations of, for example, suspected fraud, corruption, asset stripping or tunnelling, large-scale tax evasion, smuggling, grey market trading, counterfeiting/forgery, simple theft (of goods or IP, for example), money laundering, black PR, liaison with or use of organised crime gangs or any combination of these. Some of these are, in effect, specific categories of fraudulent activity, while others are not really anything to do with fraud at all; yet, when many people refer to fraud investigations, they often mean us to think in this way of a whole panoply of criminal wrongdoing which might occur within or be centred on one or more corporate entities. Asset tracing, meanwhile, in addition to encompassing a range of activities more properly falling under the banner of asset recovery, may also include activities such as people tracing and valuation of already known assets. All of the above might usefully be referred to as 'corporate investigations' and we will sometimes use this here as a catch-all term.

While fully acknowledging that it is just one piece in the investigative puzzle, the overwhelming focus of this chapter will be on corporate intelligence work. Lawyers – in many cases working closely with barristers – will often be the primary drivers of corporate investigations and the relationship between the legal and investigative teams on any investigation is crucial. At some point on almost all corporate investigations, the lawyers (external or in-house Counsel) will say, "call in the forensic accountants!", yet another shorthand used to mean a variable combination of forensic accountants, forensic technology experts and corporate intelligence specialists. Each of these have long been essential elements of most effective corporate investigations; our sense, however, is that while among those familiar with the international corporate world the roles and methodologies of the first two of these disciplines is fairly well-understood, the specifics – and importance – of corporate intelligence work are often far vaguer, and the potency of blending all three disciplines under-appreciated. In this chapter, we will seek to address some of these gaps in understanding, with reference to an array of case examples.

So what precisely is corporate intelligence, sometimes called business intelligence (in recent years, a portion of the data analytics industry has begun to refer to itself as 'business intelligence' and we have therefore come to prefer the term corporate intelligence as a banner for our own industry)? It is, in essence, a set of tools and approaches which can be applied to a wide range of investigative assignments. The investigative resources available to a corporate intelligence professional all fall into three broad categories, which we will discuss in more detail later in this chapter: a) disclosed documentation and/or electronic records; b) public records, held in electronic or paper form, whether openly accessible or available only through subscription, and, if online, whether accessible through the internet or only through a local, site-specific network; and c) human intelligence enquiries (observational site

visits also falling under this category). The maintenance of a deep and varied network of tried and trusted human intelligence sources worldwide, to be tapped into as and when needed, is thus an essential part of a corporate intelligence professional's armoury.

When considering corporate intelligence methodologies alongside those applied by forensic accountants and forensic technologists, it is helpful to recall that on any given company – and indeed on the company's individual actors – there will be both a concentrated pool of information held (for the most part confidentially) within the company itself; and a rather more dispersed cloud of information held in various forms outside the company. In the former case, various categories of relevant information can be found within a company's books and records, or reside within the heads of its employees. Forensic accountants – with the assistance of forensic technology specialists – will seek access to as large a pool of relevant proprietary information as possible. The domain of corporate intelligence professionals, meanwhile, is all pertinent information which lies outside the premises of the company and of its closest advisors – its bankers, accountants and so forth.

So let us now move on to discuss some specific types of investigations and some specific corporate intelligence resources which can yield crucial information on such investigations.

A final point before we do so. Corporate intelligence enquiries are always undertaken within a particular legal framework. This has several aspects which would each deserve detailed and complex discussion, but which are beyond the scope of this chapter. Suffice to highlight here that issues such as effective scoping of corporate intelligence work, contract terms, data protection, data security and legal privilege all require very careful attention as an underpinning to successful corporate intelligence work.

Fraud Investigation

Let us move on to discuss fraud investigations. In recent decades, the largest frauds, in terms of the sheer sums involved – at least within EU countries – have undoubtedly been the various iterations of missing trader or carousel fraud, which have cost national exchequers hundreds of billions of euros in lost VAT. These have, in their greatest part, been investigated and tackled by national tax authorities themselves, although there has been a significant role for corporate intelligence – and indeed insolvency – professionals in undertaking asset tracing work on these cases.

Procurement fraud

The classic – and still very frequently seen – corporate fraud case, though, tends to be relatively unsophisticated procurement fraud, typically involving an internal purchaser paying a party closely related to them for goods or, more commonly, services. While, on such cases, forensic accountants and forensic technology specialists are often called in, respectively, to examine relevant company books and records, interview suspects and other staff and retrieve data – notably email traffic and other messaging – from computers and other electronic devices, corporate intelligence professionals have a number of important roles to play. The latter also have the advantage of being able to proceed alone if necessary, on the basis of very limited background information.

Whether or not any more than basic identifying information is available on the key suspect or suspects within a company's procurement department and on those contractors which might be under suspicion, corporate intelligence investigators are able to undertake enquiries with the potential to bring clear and swift resolution to cases of suspected fraud. On the one hand, they might undertake integrity due diligence enquiries with the primary aim of identifying whether any of the suspect parties have any track record – ideally reported or otherwise documented in the public domain – of involvement in fraud or other malfeasance. Such diligence enquiries might, secondarily, seek evidence of potential motivation for fraud, such as indications of recent financial difficulties faced by suspects. Of equal or greater importance, corporate intelligence enquiries will seek to identify documented or reported personal connections between, classically, a procurement manager and an external contractor from which he or she has commissioned large amounts of work.

CASE STUDY 1

In a recent case in the healthcare sector, it proved possible to show conclusively that a corporate procurement manager was making heavy use of an external staff contracting firm which had not long been operating and which he himself had been instrumental in creating. Whilst any single piece of evidence might not have been sufficient proof that the procurement manager himself stood behind the company and was a likely beneficiary of it, the investigation uncovered several separate pieces of documented evidence which taken together were powerful enough for the manager to confess to wrongdoing when subsequently

interviewed. It was identified, for example, that the procurement manager was the registrant of the web domain used by the contractor company, and also that on three separate occasions in the prior decade he had – according to electoral roll data – shared a residence with the sole official director of the contractor. Moreover, the contractor shared both registered and operating addresses with a now-defunct company of which the procurement manager had been majority shareholder and director under an alias we were able to show attached to him.

CASE STUDY 2

Taking a brief step away from strictly corporate fraud, the matter of aliases was again to the fore in a bizarre case in which a lady of west African origin had been defrauded of tens of thousands of pounds by a London-based guru offering black magic 'love spells'. Following the vanishing of the cash sum, which the guru had told her to bury in a graveyard at night, and once it became evident that the spell was failing to produce the promised effect, the client found that the guru himself had disappeared from his 'consulting room', leaving us with just this address, a rather preposterous *nom de guerre* and a name which may or may not have been a permutation on his real name. His website, however, remained live. Through a mixture of company records, business and telephone directories, and – crucially – archived web pages, we were able to connect as many as 15 different pseudonyms to this same individual, including a handful of permutations of what did indeed appear to be his real name. Using the latter as the basis of our next wave of enquiries, we found that our guru had within less than a month of our enquiries been advertising services through a newly created website whose domain he had registered to what turned out to be an apartment-hotel offering short-term rentals. This information then allowed lawyers to arrange for him to be approached directly and served with legal papers, as a first step towards recovery of a portion of the missing money.

CASE STUDY 3

In a rather more prosaic case – in which, nonetheless, the fraudsters had shown a certain degree of ingenuity – there initially appeared to be a dearth of evidence that might assist investigators. Rather than a straightforward case of procurement fraud, this was a matter in which dubious procurement

was used to assist the owner-directors of a company to strip its assets. The background to the matter was potential dispute proceedings being considered by an external (creditor) party and, as the suspects still fully controlled the company concerned, there was no access possible to its internal books and records. The business concerned was a European manufacturer of high-value bespoke consumer goods with significant production lead times. The company employed a large number of skilled craftsmen and was viewed as an important employer in its locality. The client believed that the serial entrepreneurs who had bought this long-standing company a few years previously had been stripping money out of the business to fund lavish lifestyles, to the detriment of their suppliers with whom the company had begun to fall into significant arrears. Moreover, the wider economy was close to recession and the order book was looking thin.

This situation presented a new opportunity for the entrepreneurs, however: they went cap-in-hand to the regional government authority, claiming that the temporary state of the economy was threatening the company's future but that, on the other hand, its order book was starting to look better. This lobbying elicited a one-off grant from the regional authority, keen as it was to protect high-skill jobs. According to the client, though, the entrepreneurs were continuing to find ways to strip even a portion of this grant money out of the business and they asked for corporate intelligence assistance.

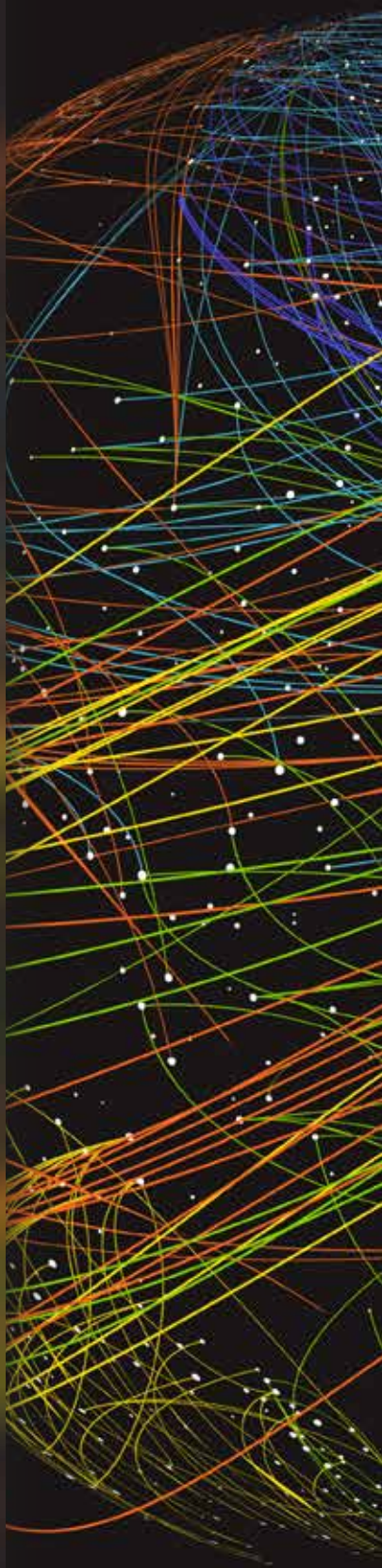
These investigations were able to assist them in three specific areas. Firstly, they were able to demonstrate from the public record that the entrepreneurs had a very patchy track record which included the collapse on their watch of two previous companies of a similar nature, manufacturing and selling high-value consumer goods. The client therefore had good reason for concern. Secondly, relying in part on a series of detailed reports by a tenacious journalist in a small local publication, supplemented with newly initiated informal but confidential enquiries amongst those familiar with the company, investigators were able to provide some assurance to the client that the company – though struggling – did not appear to be in danger of imminent collapse, and, further, that the regional authority which had provided grant money was keeping a close eye on developments. Thirdly, and most crucially, through a combination of corporate registry records across several jurisdictions, court filings and press reports going back several years, the investigators were able to show that a large order the company had received a year earlier, which had seemed suspiciously well-timed with respect to securing the grant money and which had subsequently been retracted, had come from an entity which could be considered a related party of the entrepreneurs. The order had been placed by an offshore company which investigators showed was controlled by an individual who had previously had business interests in common with the entrepreneurs, and who continued to have a residence on the same street as one of them, in Switzerland. Moreover, in their haste, the crucial large order had been made several days prior to the formal creation of the offshore company which had placed the order. All this was useful ammunition in case the client needed to proceed to taking legal action.

We should note here that this is far from the only case we have encountered in which dubious procurement has been used to assist in stripping value out of a company. In several cases of former State-owned companies across the Former Soviet states and Eastern Europe, Communist-era top managers were able to obtain majority control of large plants through privatisation deals and then proceeded to create their own personal consulting companies, usually based offshore to disguise ownership. They would then award lucrative long-term consulting contracts to these newly-created firms. Subsequent western buyers of these plants would find that not only was their financial position precarious but that the plants were locked into ruinous consulting agreements with these offshore vehicles well into the future. In several cases, corporate intelligence investigations have been able to reveal such trickery in advance of potential new purchasers of the plants taking the plunge.

Another commonly-seen scam, which again has seen core project companies leaking a great deal of money to external contractors is the use of 'ghost workers' to boost contractors' payrolls on infrastructure projects such as railway construction. In some cases, investigation work has identified the use of such frauds to be part of wider corrupt arrangements which have gone all the way to the top of government ministries.

CASE STUDY 4

Lastly on this broad topic, a case which involved nepotistic procurement practices of considerable value. A year previously, a luxury consumer goods company had hired a new executive with



responsibility for international marketing and development. This had resulted in a number of expensive brand promotion initiatives involving multiple collaborations with local agents, little-known and highly-localised luxury brands, designers and photographers. These had brought very limited value to the client's company and – following considerable investment sunk costs – the continuity of some of these initiatives was itself threatened by the precarious financial position of some of the key local collaborators. Moreover, the client had heard rumours that the executive had been forced to leave a previous role following alleged nepotistic practices. Corporate intelligence investigators were called in to assist forensic accountants working on the matter.

Corporate intelligence work first identified that several of the local contractors employed by the executive in southern Europe were owned and managed by individuals with a significant track record of failed companies. Information was also pieced together through corporate records, press reporting and residential directories to identify that in his previous role – and separately to the rumours our client had heard – the executive had controversially terminated a very large supply contract held for several years by a well-known company and instead awarded the contract in full to a new provider. This corporate intelligence work was able to show that the executive had been the key decision-maker on this contract award and that the executive's partner (who did not share his surname) at the time held an executive role at the company to which the contract had now been awarded. This, and lesser findings in a similar vein, allowed the client to confront the executive with clear evidence of a track record of wrongdoing.

Other instances of corporate fraud

Procurement is not the only function through which corporate fraud can take place of course. We will turn now to some further instances of fraudulent asset stripping by key executives of companies.

CASE STUDY 5

In the first of these cases, a lawyer-turned-tycoon in south-eastern Europe had used his connections within his country's privatisation authority to obtain control of a handful of key industrial assets across several key sectors, including power generation and shipbuilding. In this case, the client was involved in a legal dispute with this tycoon over alleged recent and ongoing asset stripping from a failing company which controlled various assets including a large industrial plant. A major part of the case centred on claims made by the tycoon, supported by written declarations from apparently relevant parties, including bankers, that he was able easily to secure investment backing for the turnaround of the plant in question. The tycoon claimed that this was logical given a claimed strong track record of business success, and that moreover he had already spent a large investment sum on taking important first steps to bring the plant fully back on-stream.

This case illustrated the importance in many instances of undertaking discreet visits to the locations of business sites in order to view their condition, signage and so on. Here an agent was sent to view the industrial plant which was manifestly in a state of some disrepair and had evidently seen no recent investment of any kind. It was completely non-operational and manned only by a skeleton security staff who informed investigators that they were owed several weeks of back pay. Further local enquiries with former workers at the site, who proved very willing to speak to the investigators, revealed considerable further detail on the recent history of the plant.

Two further sources of evidence proved critical in this case, which was in essence a matter as much of corrupt relationships with politicians, judges and key individuals within major banks as it was fraud. Firstly, through a combination of local press reports, company filings and bankruptcy court records retrieved from the archives, investigators were able to demonstrate a clear pattern to the tycoon's business track record, whereby he had obtained long-standing industrial companies cheaply through corrupt privatisation deals and then proceeded systematically to run them down, stripping out their assets and parking the cash offshore. On one notable point, investigators were able to show clear evidence that the tycoon, who claimed he had no relationship to one plant which had undergone a notorious collapse, had been its de facto owner: for example, obscure local press articles from before the collapse were unearthed reporting that he had personally entered into negotiations with workers at this plant who were striking over wage arrears.

The second of these vital sources of evidence highlighted the existence in certain jurisdictions of sometimes unsuspected public records, equivalents of which rarely exist elsewhere. Here local enquiries identified a public database which, following a number of recent banking scandals

in the country, provided a full listing of all loans above a certain value issued to companies by the country's major banks, along with the collateral put up against these loans. This database showed that the tycoon's companies had latterly secured tens of millions of euros of demonstrably corrupt loans from banks on behalf of his companies, secured against often pitiful levels of collateral: in one case, his company had received a Euro 4 million loan on which the stated collateral was a 20-year old Renault Dacia.

The careful piecing together of evidence of this track record of fraud, corruption and asset stripping resulted in the client obtaining a very favourable court judgment against the tycoon.

This is just one of many cases we have seen in which site visits – and photographic evidence from these – have made a real impact. In an oil smuggling and money laundering case, centred on a listed company which, it transpired, had no production at all of its claimed industrial goods, several of the companies in the scheme were revealed to be registered at fictional addresses, typically at non-existent building numbers on real streets. This case also involved the commonly-used tactic of fraudsters of making use of several entities with very similar or identical names registered across a variety of jurisdictions.

Other cases have involved the identification of apparently significant companies claiming to operate from sites which have turned out to be everything from a grain hopper to a tiny booth with a fax machine in an underground carpark. And it is not just particular buildings that turn out not to exist. Those with long memories may recall the famously fictional Dominion of Melchizedek, where a company at the centre of one of our fraud cases claimed to be incorporated. This was obviously a problematic place to arrange a site visit.

CASE STUDY 6

We want now to discuss another case of major fraud, involving tens of millions of euros, in which these sums were stripped out of a company through the launching of a huge – and, as investigators discovered, almost wholly fictional – special projects programme in a key Eastern European subsidiary.

The two salient features of this case from an investigator's point of view were, firstly, the ability to put together a tight-knit team including both corporate intelligence professionals and forensic accountants, and to thereby create a virtuous feedback loop: on the corporate intelligence side, information gleaned from multi-lingual public record research (corporate registry records, press reports, court records, residential records) showing numerous links between individuals who were meant to have no connection to each other was rapidly shared with the accountants, who were able to use this information to undertake key word searches on a range of disclosed documentation emanating from our client and certain external parties with which it had collaborated. Equally, this disclosed documentation contained information on budgeting and the names of external event managers used on a range of events which had been central to the special projects programme, and the accountant investigators were able to structure this as useful background information for the corporate intelligence team.

This formed the basis for the second major feature of this investigation, where corporate intelligence investigators were able in short order to arrange for a number of investigative journalists with demonstrably independent credentials to be sent on the ground in the country in question to visit the small towns where special projects events were claimed to have taken place. These enquiries involved classic reporter skills: speaking to officials at town halls and other venues at which events had supposedly been held, wider enquiries with members of the local population, taking photographs of venues and their event log books. These enquiries produced clear and consistent evidence that the great majority of the events budgeted for by the special projects programme had not taken place, and that the handful of events which had taken place had been on a scale commensurate with a fraction of the budgets purportedly allocated to them.

Further painstaking research, including through social media accounts, documented extensive cross-relationships between the various independent external event managers the programme had used and, strikingly, close ties between almost all of these event managers and a public relations firm with a dubious reputation. Taken as a whole, the investigative work pointed powerfully to a programme of high-budget fictional events having been coordinated by the PR firm on behalf of the special projects team, key members of which were each shown to have longstanding

links, dating from prior to their joining the client company, to one of the company's key executives.

Beyond fraud: other cases of corporate malfeasance

While we do not have space here to provide detailed case studies on cases of malfeasance which do not fit neatly into a definition of fraud, let us touch briefly upon a handful of examples of such investigations.

Cases of bribery and other forms of corruption are just as common as those of corporate fraud. In some of the larger corporate corruption investigations where enquiries have spanned the globe, there has been little in the way of direct and specific information pointing to the precise relationships which have been corrupt. In such cases, our remit has allowed us to undertake systematic Integrity Due Diligence exercises spanning a significant proportion of the company's global supplier base. The purpose of this work has primarily been a) to identify specific suppliers where either these companies themselves of their principals have a track record of alleged corruption, fraud or other malfeasance, b) to identify whether any specific allegations have been made publicly at local level with regard to the relationship between the company and a given supplier, and c) to identify opacity or other anomalies in the ownership structure of the suppliers. The results of this extensive due diligence work allow for the considerable narrowing down of a suspect supplier base for deeper investigation, including by accountants with access to relevant books and records. Without such a due diligence-based triage, the task facing accounting investigators would be unfathomably large.

Some cases of political corruption prove rather more tractable: in a case involving a telecoms company, we were asked by a potential investor to investigate who might sit behind a large minority stake in the company. Through examination of original paper records at offshore corporate registries in order to follow a rather long ownership chain, we showed, on the one hand, that the supposed ultimate owners were offshore lawyers. More revealingly, however, several intermediate companies in the chain had named Directors who were not offshore lawyers, and handwritten notes on one corporate file also provided us with at least one further useful name. Research of these individuals and their recent employment history pointed strongly to the ultimate owner of the stake being one or more people within the Ministry of Telecoms of the country in which the company was based, and very likely the Minister himself.

Earlier in this chapter, we made a number of references to informal enquiries undertaken by corporate intelligence specialists with a range of individuals familiar with a given company or activity. Difficult though it is to maintain these in many jurisdictions, there are certain cases in which it is vital for corporate intelligence professionals to be able to network into key areas of officialdom or specific political circles in order to gain an understanding of matters which rarely, if ever, reach the public domain. This certainly applies to cases of high political corruption but has also been important in many other types of enquiry. These have included gaining an understanding of the extent and mechanisms of corruption in customs clearance in an Asian country and also in piecing together both the networks of companies and routes used in tobacco smuggling in south-eastern Europe. Sticking with the tobacco sector, these networks were also helpful in identifying key figures behind grey market trading of large consignments of stolen non-counterfeit cigarettes produced in central Europe.

Incorporating corporate intelligence into asset tracing and recovery

As noted above, asset tracing engagements can result from any number of different contexts and are typically more aptly described under the heading of asset tracing and recovery. The oft-overlooked critical facet of asset tracing investigations is not to merely identify assets but to do so in jurisdictions where a client has a more likely chance at recovery. A US client seeking to enforce a US judgment in China against a Chinese company stands a slim chance at enforcing that judgment and getting a local court to freeze assets. If assets can be identified in the US or other "friendly" jurisdictions, the likelihood of recovery increases significantly. Using the skills of a seasoned corporate intelligence investigator, the pieces of the puzzle can be put together such that significant time and effort is not wasted in jurisdictions where the chances of success are slim.

The most common asset tracing scenarios are dispute-related, though there are times that a

corporate intelligence investigator may be asked to develop a better sense of a counterparty's asset profile in the context of a particular M&A or lending transaction. Most frequently, however, requests originate where a party may be seeking to enforce a significant judgment against another party (or parties) who claim that these assets to satisfy such a judgment simply do not exist. In other instances, a fraud or embezzlement scheme may have been uncovered and as part of the ensuing investigation, a client may need to understand just how much has been siphoned from a company and where the funds have flowed. In other instances, clients may ask for a 'lighter touch' investigation to assess the financial health and/or asset profiles for counterparties against which litigation is contemplated. Before initiating expensive and time-consuming litigation, a client may want a better understanding of its ability to recoup potential assets on the back-end of that litigation. Nevertheless, across the entire spectrum of asset tracing assignments, the core set of intelligence-gathering skills remain the same; only to be tweaked and adjusted depending on the underlying jurisdictions and circumstances.

Understanding the role of a corporate intelligence investigator as opposed to a forensic accounting expert in the context of an asset tracing assignment is often a matter of an outside-in versus an inside-out approach to intelligence gathering. Whereas forensic accountants are often working to develop insights and leads from information gained through internally held documents, discovery and/or subpoenas, corporate intelligence specialists are frequently starting their work through gathering a baseline of information in the public domain. As noted above, this intelligence gathering will be rooted in information contained in the public domain but may also include necessary colour, context and leads developed through human intelligence enquiries. In its most useful form, this intelligence can then be cross-referenced against that developed by forensic accountants or e-discovery experts working in parallel and informing each other of key links and leads that develop as a holistic look is taken at all the information gathered.

Just as the types of issues can be varied that can give rise to an asset tracing investigation, so can the types of intelligence that lead to a successful recovery. Most commonly, when asset tracing is discussed, bank accounts come to mind. Corporate investigators are frequently asked – can you get access to bank account? While the answer is most frequently 'no' for legal and practical purposes, it

should be noted that significant assets often do not sit in bank accounts. Misappropriated funds are often placed in real estate, art, yachts, motor vehicles but can also be in brokerage accounts or invested in other companies.

A successful outcome for an asset tracing assignment does not always mean that a liquid asset(s) is readily identifiable. Sometimes a trail of paper may be so complex that the value may not necessarily come in the form of identifying assets but identifying leverage against counterparties. This leverage can bring parties back to a negotiating table and/or effectuate the more rapid resolution of a dispute that might otherwise have continued for considerably longer.

A couple of case studies are included below which illustrate the manner in which useful intelligence can be gathered through corporate intelligence methods and techniques. These are by no means exhaustive but are intended to demonstrate how corporate intelligence fits as a critical piece of the overall investigations puzzle alongside other dispute services such as forensic accounting, e-discovery, etc.

CASE STUDY 7

Public record research and the importance of social media

Overview of an Ecuadorian politician tried in absentia on bribery and extortion charges

A classic corporate intelligence assignment rooted in rigorous public record research was highlighted in a joint investigation conducted by the McClatchy news organisation and *The Miami Herald*. In this case we see that the organisations, especially in an article published by McClatchy, use public record research to map a number of parties close to the target of the investigation which then leads them to transactions and entities of interest that ultimately assist them in identifying the beneficial owners of high-end real estate. As the case study demonstrates, it is typically only through being able to understand this universe of known, relevant parties that we can understand the context behind certain transactions that ultimately lead to the identification of key assets and also parties critical to facilitating the movement of illicit funds and their concealment.

These publications focused on events surrounding an Ecuadorian politician, Carlos Polit, and his son John Polit; both of whom were sentenced in absentia by the country of Ecuador for partaking in a bribery and extortion scheme. Carlos Polit was charged with extorting bribes from the Brazilian construction giant Odebrecht for certain infrastructure projects in Ecuador. The articles identified ownership interests in high-end Miami, Florida real estate with an estimated market value, at the time, of over USD 7 million which are believed to have come from the proceeds of this bribery scheme. According to the articles, Carlos Polit had been accused of taking USD 10 million in bribes and was on the hook for over USD 40 million in restitution as a result of his being found guilty at trial in Ecuador.

It is important to note that the South Florida area in the United States has long been an attractive destination for politicians, businessmen, drug lords, etc. seeking to park ill-gotten gains in luxury real estate developments where it is easy for the beneficial ownership of the properties to remain opaque. While the scrutiny around anti-money laundering requirements and identification of beneficial owners has been gaining momentum in Florida and the United States, it was often the case that purchases in this market were made through off-shore shell companies or through Florida limited liability companies where the beneficial owners were not required to be disclosed.

McClatchy claimed that its investigation had identified approximately USD 7 million in real estate purchases made by certain limited liability companies in cash that were ultimately traced to the Polits. In the United States, these cash purchases meant that no mortgage was required when the properties were purchased, and thus no disclosure regarding ownership. However, mortgages were later taken out on these properties which contained the name of Carlos Polit's son, John, in certain instances. It was at this point that the paper trail could be examined which ultimately not only identified the underlying properties but related individuals and entities to be examined in further detail as they were critical to facilitating the movement of funds and identifying their footprints would lead the investigators to other assets as well.

The importance of social media in connecting the dots

The skills used by the investigators from McClatchy and the *Miami Herald* on the engagement were applied in much the same way a corporate intelligence investigator would. At the outset, their public record research noted that there were no properties in Carlos Polit's name, nor was he listed as an officer or director for any

entities registered in Florida. They had identified a LinkedIn profile for John Polit which said he worked in real estate in Ecuador but their research identified a public disclosure form that showed John Polit was working at Merrill Lynch in Miami as a financial advisor until mid-2018 which is around the time he faced his significant legal troubles in Ecuador. More importantly, they identified a Facebook profile for Polit from which they were able to extract details about his "friends".

Social media has increasingly become a critical tool in asset tracing assignments. It may show critical connections between individuals that would otherwise go unknown. It can help establish timelines and travel habits. It can frequently even identify assets as individuals are often eager to take a picture of a new car or sailing on their new yacht.

While most Facebook users are increasingly wary about keeping their privacy settings low and limit the visibility of their posts, a large number still make their friends lists completely available. This information can be valuable in any number of ways but copying the names into a spreadsheet so they can be matched against other relevant data at a later point can often be a useful step. More on this to come below.

Examination of information available in the public domain – corporate registry details and property records

In the United States, property records are often available through desktop research. The information may include not only the current owners of the properties, but also the deed history which will detail the changes in ownership and mortgage history for the property. The ability to interrogate property records varies by jurisdiction, but in the case of Miami-Dade County in Florida, a researcher can run searches by individual name (not just on the address itself) as well as running searches for a particular address.

As noted above, the Polits had not taken a mortgage out at the time several properties were purchased and were nowhere to be found in any of the related documentation. At a later date, however, John Polit took out a mortgage on one of the luxury properties for USD 1.7 million. By doing so, John Polit had inserted himself into the public record and the McClatchy investigators had the one string they needed to pull that would ultimately lead them to understanding the bigger picture.

The documents are publicly available online and show John Polit signing the mortgage documents as the sole member of 8112 Los Pinos Cir, LLC (an LLC created for the ownership of the property located at this address). When one searches the Florida corporate registry records, however, John Polit is not listed as an officer, director or registered agent of any LLCs and not 8112 Los Pinos Cir, LLC despite being referenced as a managing member in the mortgage document.

The next logical step was to conduct a search of the corporate registry records to see who was listed on the documents for 8112 Los Pinos Cir, LLC. Perhaps not surprisingly, John Polit's name was not listed on these records, but the searches did reveal a number of names on the documents that were Facebook friends with John Polit. Now, armed with the insight into the possible individuals who might be being used as proxies by the Polits, the McClatchy journalists were able to identify a number of Florida LLCs, most of which had managing members and directors that were John Polit's Facebook friends.

Using the public record to identify proxies, leads and, eventually, other properties

A review of the property records for the 8112 Los Pinos property showed that the agent listing the property was a young broker in the Miami area who hailed from the same part of Ecuador as the Polit family. A later change to the 8112 Los Pinos Cir, LLC records inserted a second individual into the role as a Managing Member who served the same role on another LLC created for a property where John Polit later took out another mortgage. A third property was identified where John Polit had signed as the guarantor on yet another mortgage. This time, another individual is listed on the associated LLC for the property which does not list John Polit. The individual was cited on additional LLCs set up to hold properties as well. While all the subsequent details of the real estate findings need not be detailed here, the work is illustrative of exactly how corporate intelligence is used at the beginning of an investigation to put the pieces of the puzzle together. The McClatchy team had just started to pull on this one string to see what was there and identified key real estate assets and an apparent network of individuals that were used as cover for the initial purchases and to disguise the beneficial ownership.

It should also be noted that, according to the McClatchy report, none of the properties it identified were part of the Ecuadorian government's prosecution against the Polits. The report is a

useful tool in understanding how Florida Limited Liability Companies can help disguise or obscure beneficial ownership but also how those same records, when carefully pored over, are a critical piece of the puzzle that corporate intelligence specialists use to connect the relevant parties.

CASE STUDY 8

Link analysis and visualisation platforms as a key corporate intelligence tool

When conducting the type of research described above, one can amass significant amounts of records containing names, addresses, phone numbers, shareholding details, etc. The amount of data can quickly reach a point that even the best and most experienced corporate intelligence investigators cannot simply connect the dots based on their memory alone.

The visualisation platforms on the market are often useful for clearly displaying relevant connections and timelines that would otherwise be difficult to understand in a narrative form. These tools typically sit on top of a robust link analysis platform that can ingest all of this data and make the connections across the high volume of data that would otherwise not be spotted by the naked eye.

The most advanced of these platforms can not only make the connections across all the public record research gathered but can also be integrated with e-discovery platforms and other databases so that the intelligence gathered from the outside-in can be cross referenced against the data gathered from the inside-out.

Link analysis and human source inquiries – A case study in China

A client was seeking to enforce a judgment against a company in China and would have considerably more leverage in pursuing its claim if it were able to connect the dots amongst certain companies that had exposure in overseas markets where the client could more easily seek to enforce certain remedies. Specifically, the client wanted to tie the counterparties to certain goods that had been shipped to California which were of a significant value. The client hoped to show that transactions relating to these assets were not conducted at arms-length and could then seek to freeze these particular assets in an effort to satisfy the judgment.

An initial look across the various entities in China did not show any obvious points of overlap when it came to officers, directors, shareholders, office locations, etc. The companies appeared to be trading partners and the preliminary public record research in China did not show any obvious connections between the companies other than their normal course of business commercial interactions.

It should be noted that corporate registry details in China are fairly accessible, especially relative to other countries in the region. The country has a relatively decentralised process under the State Administration for Industry and Commerce (SAIC), which means that the types of information contained may vary somewhat from province to province or municipality to municipality. On the whole, however, the records are fairly complete and typically will contain a current list of officers, directors and shareholders. These records frequently also demonstrate changes over time so one can see how the shareholding structure has evolved and whether new directors have been added or removed over the years.

In the case of seeking to establish links among these dozens of companies, the corporate registry information – along with all the historical information – was gathered and imported into a link analysis platform. The platform was very quickly able to sift through all of the data (using both the Chinese characters and their Latin character transliterations) and identify certain points of commonality amongst directors and earlier cross shareholdings of particular interest. As further research was conducted on the new entities that entered the shareholding structure, it became clear that the company had created a complex shareholding structure that appeared to connect a number of the relevant entities of interest.

In parallel, research was being done in the United States to gather information on the California-based companies holding these assets which needed to then be connected back to the companies in China. While corporate registry details for private companies in the United States are nominal relative to such companies in China, litigation filings are more readily available in the US which provided key investigative leads from a review of these documents.

Research identified a number of wrongful termination lawsuits that had been filed by former employees of the California-based companies that were of interest. A review of the records showed several employees claiming that they had been long-term employees of the company but had been forced out of their jobs when management brought over managers from China to take their roles. As any corporate investigator

is well-aware, a disaffected former employee can always be a treasure trove of great intelligence.

In this case, the former employees' current whereabouts were identified, and several were approached for interviews. When asked if they could help with identifying the owner of their past employer, a couple of the employees were eager to explain that the true owner of the company was not the individual identified on certain corporate filings but to the owner of the China-based companies of interest, explaining that he used to visit the companies quite frequently.

The former employees were able to provide more detail into these transactions at less arms-length and even pointed investigators to a warehouse where all of the goods were being shipped though they were not ending up with end-users. The goods were simply being kept in these warehouses to hide the fact that they were not being shipped to true end-users at market rates.

In this case, while the public record did not support the links that the client needed to make, human source intelligence was the key to establishing that link and ultimately showed that certain transactions were not made at arms-length and were ultimately indicative of stripping a company of certain assets so that creditors could not lay claim to them.

Range of resources

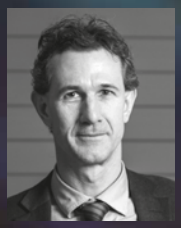
In conclusion, corporate intelligence professionals have a very wide array of investigative tools at their disposal. Discounting an inevitable dimension of luck, their success will depend in large part on their ability to access, make effective use of, and usefully combine all such resources which may be relevant. Access to such resources aside, this work puts a premium on acute analytical skills, effective communication with clients in order to agree on relevant and achievable objectives, and the interpretive ability effectively to frame important findings within the relevant context: sectoral, political and so forth.

A premium should be put on identifying corporate intelligence investigators with a keen understanding of the operating environment which includes the composition and availability of the types of public records critical to an investigation. An experienced corporate intelligence investigator should be aware of the difference in the types of records available online through desktop research and through on-site searches in hard-copy form.

We have highlighted through case examples several categories of electronic and paper-based public records which may be tapped, and there are others which we have not had the space to mention; particularly where cases touch upon high-profile individuals, for example, or where it is important to understand local deep state or crime gang structures, hard copy academic books and journals can be of considerable importance.

With regard to human intelligence source enquiries, we have touched upon networking into relevant business, political and bureaucratic circles, and on the use of investigative journalists, as well as more straightforwardly observational site visits. But there are investigations on which other categories of network need to be tapped into (Israeli kibbutzes, in one recent example), and industry sector expertise is often vital in allowing effective interpretation of findings such as the *modus operandi* behind a fraud scheme or key proxies used to conceal the movement of ill-gotten gains.

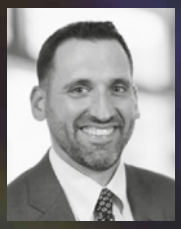
Where technology is positioned as integral to these types of corporate intelligence efforts, a distinction should be made between those technology tools that appear to aggregate superficial information more quickly and those tools that genuinely add an extra research or analytical dimension to an experienced corporate investigator's powers. CDR



Alexander Davies is BDO UK's head of corporate intelligence and has spent 25 years as a dedicated corporate intelligence professional.

Following two years working in the international investigations team at specialist firm Control Risks, in 1997 Alex became one of the two co-founders of the first corporate intelligence team to be created within any of the major accounting firms anywhere in the world, at Deloitte in London. Latterly he was director of this team and was instrumental in building it into a team of 30.

alexander.davies@bdo.co.uk



Peter Woglom is a managing director in BDO USA LLP's Forensic and litigation services practice. Peter began his career at Kroll later working for Control Risks and Deloitte, where he and Alex worked together on a number of high-profile investigations over the course of several years.

Peter focuses on intelligence gathering for complex M&A engagements, dispute matters and asset tracing/ recovery assignments.

Peter received his Bachelor of Arts from Claremont McKenna College and an MBA from Emory University's Goizueta School of Business.

pwoglom@bdo.com

BDO's corporate intelligence team forms part of the firm's Forensic Practice. In the context of 'reactive' investigations, such as those concerning suspicions of fraud or other malfeasance, the team frequently works in tandem with the adjacent forensic accounting investigations and forensic technology teams, and also on occasion with the firm's appointment takers with a contentious insolvency specialism. With respect to more 'proactive' integrity due diligence work, the corporate intelligence team instead links more often to various parts of our corporate finance practice.

Although the team's skills may be called upon in numerous other contexts, most frequently our corporate intelligence experts gather information on individuals and entities in the context of contemplated business relationships or transactions, fraud and corruption investigations, asset tracing, litigation support and other disputes. The team works worldwide on behalf of global financial institutions, law firms and corporate clients, developing insight and intelligence through a robust review of information available in the public record and, when necessary, through our external network of expert, local sources.

www.bdo.com

Data analytics and data visualisation in asset tracing:

Evolving approaches to transaction analysis and communication

Andrew Maclay
FRA

Matthew Rees
FRA

Mason Pan
FRA

"Where has all the money gone?" is probably the most important question in asset recovery. This is swiftly followed by "How can we get it back, and who can help us?" In the old days, legal teams helping their client recover assets would obtain 50 boxes of documents from banks and turn it over to a forensic accountant. The information contained within these banking documents would then be manually entered into spreadsheets by inexperienced staff. Linking the disparate information in order to trace funds through correspondent bank accounts and offshore trusts was a very time-consuming and difficult exercise.

Furthermore, given the manual nature of the work and high volume of information, the identification of patterns and finding leads were often the result of pure luck and the good memories of the team members. Today data analytics and data visualisation techniques can transform how efficiently and effectively the tracing team can overcome the other side's diversionary tactics and track down the stolen assets.

In this chapter we explain how modern data-driven techniques are enhancing the established art of *"following the money"*: how the already well-honed techniques of evidence collection and a multi-disciplined, multi-jurisdictional team can reap the benefits of new tools and technologies.

The information challenge

Asset tracing is a painstaking task. Through a breach of trust or other dishonest act, assets are taken from an organisation, most often in the

form of a series of high-value bank transfers, and then rapidly dissipated through the international banking system into offshore trusts and valuable property. The challenge for the legal and forensic accounting team is to identify the location of these assets which may be controlled from fiscal paradises, in accounts in the name of trusts, in shares in offshore companies, in physical property and even yachts in far-flung jurisdictions. The ownership of such trusts, companies and property is often made deliberately opaque to hinder identification and recovery.

Three factors add further difficulty to the challenge. The first is the problem of the moving target. Assets can continue to be moved from jurisdiction to jurisdiction while the team obtains compelling evidence to gain court orders to freeze them or subpoenas for more information.

Second, the evidence itself must be obtained from jurisdictions where achieving the necessary disclosure of information is hard-fought. In some jurisdictions the challenge is exacerbated by under-resourced authorities and even local corruption, particularly where the State has been involved in the asset misappropriation.

These two factors result in a process in which new material is constantly added, requiring the corpus of data to be updated iteratively while duplicate or contradictory information is detected. A well-designed evidence collection and data analytics process is ideally suited to these tasks especially where time is of the essence to have a chance of prosecution or recovery of assets.

The third factor is the relentless innovation that characterises the financial services industry. Near-instantaneous funds transfer and the emergence of crypto-currencies are two examples of developments that make the task of asset tracing more challenging.

Establishing a central repository of information

The foundation of successful asset tracing is the effective management of evidence through a comprehensive information management strategy. Information is likely to be received sporadically and in many forms. It will have to be converted and interpreted swiftly and accurately.

Moreover, the variety of information sources and data types is also increasing. Historically-used sources, such as emails, bank statements, transactional data, accounting records and contractual information, needs to be combined with newer intelligence sources such as social media networks and activity, mobile phone records and IP address data from remote log-in events. Knitting together these pieces of information helps to paint the picture – identifying individuals instructing the transfers, the described purpose of the transactions and other contextual details. However, to extract additional intelligence and further extend the range of the asset tracing, such details need to be matched to individual transactions and then be closely examined.

To start building this picture, information must be gathered and stored in a central repository and digitised, if necessary. This repository must be capable of accommodating and integrating data from disparate sources that could be delivered in a multitude of formats including both structured data (e.g., banking transactions spreadsheets and accounting systems) and unstructured data (e.g., emails, PDF bank statements, account opening documents, corporate records and transfer instructions).

Another essential consideration is data privacy and protection regulations. Given the multi-jurisdictional nature of asset tracing, it is critical to develop effective data governance protocols in the intake and storage of received data in order to comply with international data protection regulations (e.g., the EU's GDPR) and country-specific statutes (e.g., China's State Secrets Law). Failure to do so can result in harsh penalties or a damaged reputation. Therefore, in certain situations, it is not possible to establish a single central repository, so careful thought must be given to mitigate operational and regulatory risks.

Taking all this into account, having a well-designed, comprehensive and up-to-date information repository is a key prerequisite for the deployment of advanced data analytics.

Preparing the data for analysis

In order to track the passage of cash as it moves through the global banking system, the key data processing activities are data conversion and data standardisation. There are a wide range of tools and techniques available to perform these activities.

Ideally, relevant information such as bank transactions will be obtained in electronic form. For this the process of transfer into the database

is relatively simple. However, information may also be provided in the form of hard copies or scanned images, in which case they must be converted using tools such as Optical Character Recognition (OCR) software. These technologies have continuously evolved so that documents such as bank statements can swiftly and accurately be scanned, converted and validated into structured formats with limited manual intervention beyond set up and quality checks. Once this is complete, the data is loaded into the database and the data can be assessed for standardisation needs.

Data standardisation is a critical activity as the same type of information (e.g., bank transactions) could be received from different sources and contain different formats, codes, languages, quality and levels of detail. As such, the data will need to be standardised into a single format, which enables the investigator to holistically review the disparate pieces of information. An experienced data analyst can efficiently review the data to determine the extent of standardisation that is required. Judgment will be required and the analyst should prioritise data fields from the disparate data sources where standardisation enables the data linkages to be made.

Other documents such as emails and attachments, which may be in hard copy or electronic forms, should normally be converted and uploaded into an eDiscovery review platform. While metadata is likely to be readily available for electronic documents, hard copy documents will require more manual work to determine information relating to their provenance and authorship.

Irrespective of the source of the documents, developments in the automation of document identification and the extraction of intelligence mean that the deployment of new technologies at this stage can save a great deal of time. With this aspect of the matter more efficiently addressed, the investigator is free to use their skills and experience to execute the overall asset tracing and investigation strategy.

Combining structured and unstructured data and the use of artificial intelligence (AI)

Over recent years, one of the most significant developments in investigations, including asset tracing, has been the ability to effectively and almost seamlessly combine structured and unstructured data within an investigation. The objective of this integration is to enable the investigator readily to access details of a transaction alongside documentary evidence that has been collected and identified as relating to the inception, purpose or rationale of that transaction.

Careful design of the review platform can enhance the ease with which forensic accountants and lawyers work through the information. However, beyond simply improving the quality of the forensic accountant's interaction with the data, AI can be used to automatically suggest matches between communications and documents with specific payments and receipts. In this context, AI is intelligently comparing key pieces of information such as companies, individuals, dates and amounts with all other pre-existing data in the possession of the investigator.

To illustrate this concept, consider the example of dealings in a property in Ukraine for which some documents have been disclosed and processed into the data repository. Analytical processes may, through identification of dates, prices and addresses within the document, infer that the property may have been purchased using funds that were transferred out of Dollar or Euro denominated bank accounts in Cyprus and the British Virgin Islands. This could be achieved by a data analyst configuring the algorithms and parameters to look for matches based on date ranges, exchange rates and company information.

Even where the complexity or obscurity of the transaction defeats the matching algorithms, powerful search capabilities and intuitive user-interfaces can ease the matching efforts. In some cases, the system can be programmed to provide a range of 'best guess' alternatives for human validation.

Automating the tasks

All of the hard work and time invested in designing and building the digital repository pays off when it comes to tracking the movements of funds between the bank accounts and into the destination assets. Modern techniques can simply automate what were previously repetitive tasks. This means that through collaboration between the forensic accountants and data analysts, the tracing can be accomplished faster and with more objectivity.

For example, the date and amount of a payment may not exactly correspond with the date and

Irrespective of the source of the documents, developments in the automation of document identification and the extraction of intelligence mean that the deployment of new technologies at this stage can save a great deal of time

amount for that same transaction that appears in the receiving bank account. Differences in the value date, changes in currency and the imposition of bank charges can inhibit exact matching, especially in situations where there are many payments of similar value taking place within short timeframes.

Using data analytics techniques, transaction value and date matching tolerances can be programmed so that matches can be suggested where the recorded dates vary by a few days, values differ by typical bank charge amounts or by taking into account variations in exchange rates. Matched results can be assigned confidence scores to help investigators in their review. Paired entries which have been detected using matching algorithms can be presented, along with supporting linked documents, to the investigator for final validation.

Further, the information may point to a single payment being split at some intermediate stage before being credited to multiple accounts. Under these circumstances, database queries can be created to iteratively seek out and test the many permutations and combinations such that the most likely transaction flow is identified.

Using data analytics to further enhance the skills of the investigator

One of the key challenges that arises is when funds move into accounts which already contain other, potentially unconnected funds or which are overdrawn. The challenge is how to treat subsequent payments out of the account containing the mixed funds or, indeed in the latter case, the earlier payments which caused the overdraft in the first place.

The interpretation may be subject to strict rules which the defendant may use to their benefit. For example, in the UK, the extent to which the funds paid out from the receiving account can be treated as trust assets may be determined by applying the appropriate legal rules of tracing. Such rules are required where, for example, an intermediate account already contained non-trust funds or was overdrawn prior to receiving the claimant's funds. While the detail of such rules is outside the scope of this chapter, data analytics provides an opportunity to adhere to such rules more efficiently.

Encoding the legal tracing rules into automated routines and algorithms has significant benefits to the effectiveness of the investigation. First, once translated into database scripts, the rules are consistently applied across all transactions and replace considerable manual effort and subjectivity on the part of multiple investigators. Second, as further information is added to the data repository, the routines may be re-run and the revised money flows revealed almost instantly.

Similarly, the effect of assumptions as to the source of certain funds or the destination of particular payments may be tested. In this way, investigation efforts may be directed at the areas which are likely to yield most benefit in terms of the identification of the greatest value of assets for recovery. For example, where an account receives a large credit from an as yet unknown source, the impact of assuming that the source was in fact trust assets can be tested. If such an assumption yields an increase in value of recoverable trust funds, a decision may be made to deploy more investigative efforts to determine its true source. Conversely, if the effect is small, the investigator may decide that their time is be better spent examining other branches of the transaction flows.

A further related benefit of using data analytics to track the flow of funds is the identification of repeating patterns of transactions. When fraudsters alight upon a mechanism that works, they

will often repeat it. This repetition may be in the form of combinations of money flows between particular jurisdictions, the acquisition of certain types of asset and the use of more complex arrangements such as back-to-back loans. Data analysts can write programs to identify such patterns and repetitions and save the investigator a great deal of time and effort.

So, data analytics and the automation of the data matching mean that time is saved and payments can be linked with greater objectivity, but more importantly the investigator can concentrate on understanding where the money has gone and critiquing the links between entities and transactions that are suggested by the machine analysis.

Uncovering the networks using data visualisation

One of the areas where there has been a proliferation of technological advances has been data visualisation, and it is here that the effects of applying technology will, by definition, be most visible. As much of asset tracing is based on interpreting transactions as flows of funds and identifying hidden links between individuals and entities, such data visualisation can be incredibly valuable to the investigator.

We illustrate how the underlying story of the asset flows may be told with four types of visualisation techniques.

Link charts

On the most basic level, building up link charts such as i2 showing the source and destination of each funds transfer has historically provided an effective way of tracking progress. These will be familiar to many as they have been used for years in both analogue and digital forms. A link chart uses a variety of icons to depict bank accounts, trusts, property and valuable items such as aircraft and cars. Each item depicted by the icon is associated with a virtual index card which contains all the information known about that entity, or indeed the transfers of money into it.

The investigator is able to use such charts to identify the current-state extent of the intelligence extracted from the information and determine the end-points on which to focus investigation efforts. Further, link charts may be used to understand and depict the other linkages between entities – such linkages may include common ownership and connected individuals such as legal or financial advisors or addresses.

Geographical map

Another simple, but effective approach to illustrating the flows of funds is to overlay them on a geographical map – drawing on the metadata surrounding the individuals, companies and bank accounts. In this way key jurisdictions where the activity takes place are readily identifiable.

Amongst the variety of other less conventional visualisation methods that are available today, we will highlight two techniques which lend themselves well to asset tracing: *Sankey* and *Chord Diagrams*.

Sankey diagrams *(see Figure 1)*

Designed by Captain Matthew Sankey in the nineteenth century to illustrate the energy efficiency of

When fraudsters alight upon a mechanism that works, they will often repeat it. This repetition may be in the form of combinations of money flows between particular jurisdictions, the acquisition of certain types of asset and the use of more complex arrangements such as back-to-back loans

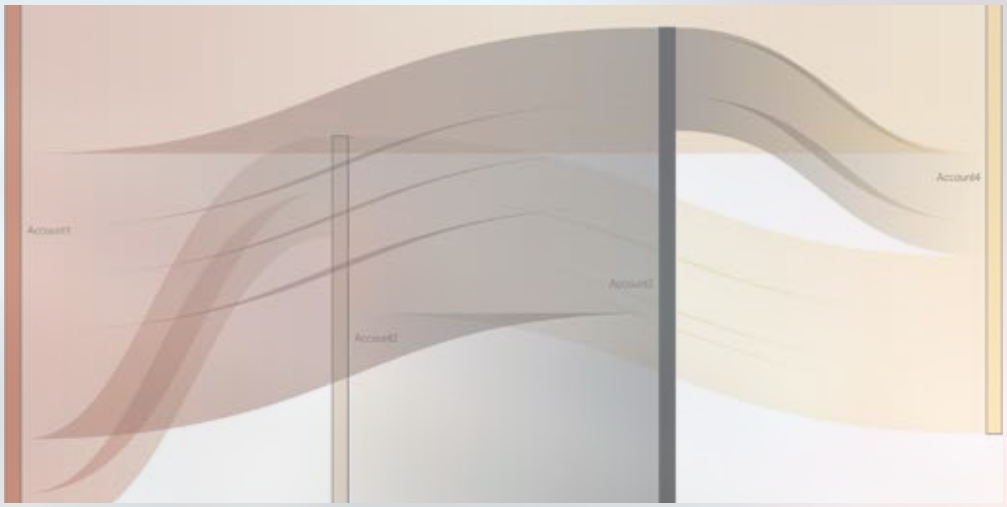


Figure 1 - example of a Sankey diagram

a steam engine, Sankey diagrams are a type of flow diagram in which the strength of linkage between two entities is depicted by the thickness of the interconnecting line. In their twenty-first century form, these charts are interactive such that the connections can be explored and the source and destination of assets can be tracked and demonstrated through multiple intermediate stages.

Chord diagrams *(see Figure 2)*

This type of visualisation, also known as a Hierarchical Edge Bundling chart, is another way of depicting the extent of flows and linkages between entities. Chord diagrams are named after the line which connects two points on a circle.

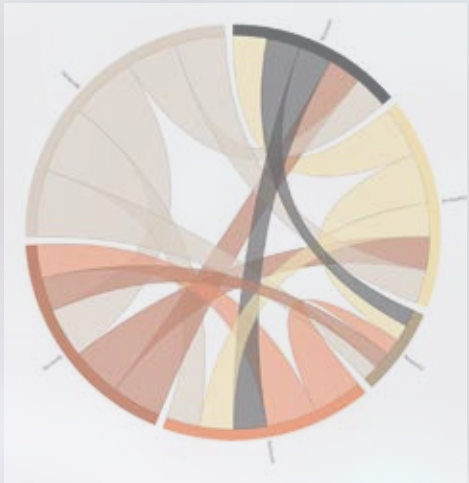


Figure 2 - example of a Chord diagram

Edge bundling is a technique for combining similar end points, such as bank accounts or corporations, to simplify and make such visualisations more useful. Again, the charts are interactive and enable the investigator to explore the linkages and gain an alternative perspective that may elude them when examining tables of data or link charts.

If these types of visualisation do not suit the specific situation or the investigator's preferences, there are many more that can be easily connected to the underlying investigation data repository irrespective of the underlying database. Whether they are a stand-alone tool or from an open-source, there are libraries of pre-built visualisations that are designed to be displayed and to enable interaction with data in any web browser.

Whatever the intended output, the key to enabling the use of all of these visualisations is the design of the digital repository. It is essential that the information store is configured in such a way that it is capable of supporting the intended outputs.

Dashboards

All of the hard work and ingenuity that we have described in this chapter would be wasted without an effective interface between the data and the human mind. In this context, dashboards are user interfaces which enable the investigator to easily peruse the data, drill into specific transactions to examine the underlying evidence and tweak assumptions at the click of button. Typically

delivered through a web-browser so that teams can be distributed between firms and jurisdictions, such dashboards may be customised to match the needs of the case and even those of each type of user.

As we have explained, one of the main benefits of data analytics and data visualisation is that the investigator can apply a range of assumptions and examine their effects. The dashboards are designed to be interactive, enabling a non-data scientist to effectively work with the information. Filters are used to change the views, date ranges or specific entities may be selected and the visualisations programmed to change in response. The user may drill down on specific transactions to view the associated documents and even add details and record inferences.

To achieve this interactivity, the dashboard brings together many of the features described previously: for example, data visualisations illustrating the flows of assets, simple lists of transactions and panels displaying related documents such as bank statements or emails.

Presenting the findings

Historically, the output from an asset tracing exercise was presented to courts in long written reports carefully narrating each transaction and the associated evidence. Such reports were accompanied by static charts which reflected the effect of the reported transactions.

The clarity and usability of the outputs from asset tracing investigations has been transformed by the use of interactive visualisations and dashboards of the type described above. The effectiveness of the presentation of the facts of the case is enhanced and the networks of asset flows and entities may be explored and reworked by the parties or the judge as the matter proceeds and more evidence is uncovered. It may be that the best way of presenting the findings of an asset tracing case, today or in the future, is by way of live modelling of the data in a courtroom, using data visualisation tools – with all the flexing of the model fully explained by the operator, and with the model and assumptions disclosed to the other side, so that it can carry out its own testing and validation.

Conclusion

As we have explained, the core challenges of asset tracing remain managing and interpreting large volumes of disparate data, to achieve the overall goal of finding and recovering the assets. What has changed is that both the volume of data and the variety of data sources have increased alongside relentless innovation in financial services and payment processing. Helpfully, technologies have been developed that enable the forensic accountant to better meet these challenges. With careful planning and an integrated multi-disciplinary team, effective and efficient asset tracing can be achieved. The key aspects of such an approach include:

- The integration of structured and unstructured data to enable seamless switching between transactions and the underlying documents and the provision of this information through interactive dashboards and eDiscovery platforms.
- Exploiting data visualisation techniques to portray transaction flows and asset movements in a way that enables better assessment of the evidence and communication of the findings.
- The use of advanced data analytics to automate repetitive matching tasks and uncover hidden connections between transactions, events and entities.

But it is important to recognise that such an approach does not replace the requirement for the investigative skills of the forensic accountant. Rather, the use of technology should be seen as an enabler – providing the investigator with the time, space and facilities to deploy their own, unique skills to answer the question of "Where has all the money gone?" and help to recover assets for their client.

Andrew Maclay specialises in acting as an accounting expert in international arbitration and asset recovery cases. Andrew was the forensic accounting officer of the IBA asset recovery subcommittee, and over the last 20 years, Andrew has worked on many large asset recovery cases including in relation to General Abacha in Nigeria, the Versailles Group, a Saudi businessman and a Milan corruption investigation where he was appointed special representative in the UK for an Italian magistrate. He has acted on investigation and arbitration projects in the UK, France, Switzerland, Kenya, Nigeria, South Africa, the DR Congo, Romania, Albania, Bosnia, Kazakhstan, Egypt, Indonesia, India, Qatar and Saudi Arabia, amongst others. He has also acted as an expert on quantum and all types of accounting disputes, including the interpretation of international accounting standards in breach of contract, breach of warranty and expert determination disputes. Andrew is accredited by the ICAEW and the Academy of Experts as an accounting expert. He has been recognised as an expert in many *Who's Who Legal* (WWL) publications, including *WWL Asset Recovery, WWL Investigations, WWL Arbitration* and *WWL Consulting Experts*.

amaclay@forensicrisk.com

Matthew Rees has more than 20 years' experience of delivering forensic accounting, data analytics and internal audit services. He has experience of a wide range of industries including banking, pharmaceuticals, telecommunications, oil and gas and fine art gained in many regions including Africa, Central America and the Middle East. Prior to joining FRA, Matthew spent five years in the Internal Audit team at Citigroup where he was responsible for providing assurance over fraud risk and designing and implementing audit programs and enabling tools. In addition, he conducted investigations in response to concerns escalated by regulators and through the bank's own ethics reporting channels. Throughout his career Matthew has designed and delivered training programmes on fraud and forensic technology. He has published articles on forensic accounting in general and the application of technology in particular and he was the contributing editor of the book "*Corporate Fraud – The Human Factor*" (Bloomsbury, 2014).

mrees@forensicrisk.com

Mason Pan delivers analytics-led solutions to global corporations and law firms to help them respond to business-critical events by identifying, quantifying and mitigating risks. He specialises in cross-border and multi-jurisdictional investigations and compliance matters.

Mason helps his clients assess allegations of misconduct and respond to regulatory investigations by applying data analytics to narrow the investigative focus, map relationships between disparate systems and identify data patterns and irregularities to derive conclusions based on electronic evidence. He also provides risk assessment, litigation and disputes consulting services and has extensive experience with compliance monitorships post government settlement.

On the proactive side, Mason helps enterprises design and implement analytics-led compliance monitoring and anti-fraud/bribery/corruption solutions to enable enterprises to continuously detect, understand and manage their risks while complying with new regulations and enforcement activity.

He has worked in industries including financial services, manufacturing, mining, oil and gas, pharmaceutical, transportation, and software/high-tech.

mpan@forensicrisk.com

FRA is an international consultancy specialising in regulatory cross-border, multi-jurisdictional investigations, compliance and litigation. We are expert providers of forensic accounting services, data analytics and data governance, technology solutions and forensics. Unlike traditional accounting firms, we do not perform audit or other consulting work, so we typically have no internal conflicts. Our offices are in the US, the UK, France, Finland, Sweden, Canada and Switzerland. With over 20 years of experience, we are known for delivering bespoke solutions around the world for complex and highly sensitive matters and are experts in analysing large, complex transactional data sets. We also offer jurisdiction-specific consulting services on data protection, blocking statutes, state secrecy and cyber laws. We have state-of-the-art data centres that meet or exceed Tier III standards in Canada, France, Sweden, Switzerland, the UK, and the US.

www.forensicrisk.com

Bermuda

Mathew Clingerman
KRyS Global

Bermuda is the oldest self-governing British overseas territory with a long history of upholding the rule of law. Its legal system is derived from English common law and unsurprisingly much of the Bermuda legislation is modelled on English statutes.

Bermuda has been a pioneer as an offshore financial centre since the mid-1960s and has an enviable market reputation based on attracting quality international business. Often referred to as the "risk capital of the world", a significant percentage of the world's largest reinsurers are based and have operations in Bermuda. Notably, however, its active corporate registrations number is less than 20,000. The local financial regulator, the Bermuda Monetary Authority, also plays a strong role in ensuring the compliance of businesses that carry on regulated activities across the areas of insurance, banking, investment funds, fund administration, investment business, trust, corporate services, money services, and digital assets.

Notwithstanding Bermuda's focus on quality, inevitably bad actors can make their way into the system as they do in any financial market. When this occurs, it is not uncommon to see negative headlines that contribute to a misguided perception that Bermuda is a jurisdiction cloaked in secrecy that exists only to facilitate money laundering, tax evasion, and to stash ill-gotten gains. In truth, Bermuda is a jurisdiction that boasts more transparency than most onshore jurisdictions, is known as a first adopter of international standards, has a history of proactive regulation, and is supported by robust judiciary together with a capable and sophisticated local legal profession.

As an offshore financial centre, most frauds or financial crimes that touch Bermuda involve wrongdoers located outside of the jurisdiction. Consequently, most fraud, asset tracing, and recovery exercises have substantial cross-border aspects. Fraudsters rarely use Bermuda simply to stash large bank deposits or other assets. In many cases, the wrongdoers seek to integrate the proceeds of their fraud back into an onshore financial system giving an appearance of legitimacy. The proceeds are also frequently used to fund a fraudster's lifestyle such as purchases of luxury homes, private planes, yachts, or even expensive private education.

When fraud matters do arise there are wide array of remedies and relief available in Bermuda to victims seeking redress. Time and again, the Bermuda judiciary has demonstrated its commitment in these cases to obtaining justice. The strength of this system is one of the underpinnings that give confidence to investors and financial participants in Bermuda's market place.

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

Judiciary

The Supreme Court of Bermuda (the "**Bermuda Court**") has both civil and criminal divisions. It is a court of first instance for all civil disputes concerning a value greater than $25,000. The commercial court division of the civil division will comprise judges experienced in complex disputes involving, among other areas, trade, commerce, insurance, banking, and financial services. The Bermuda Court is served by a Chief Justice, three puisne judges, and a panel of assistant judges which ensure cases are moved along expeditiously.

The Bermuda Court of Appeal, consisting of a three-judge panel, meets three times a year to hear appeals of the Bermuda Court's decisions. Further appeals may be heard by the Judicial Committee of the Privy Council in London ("**JCPC**"). Any decisions of the JCPC in relation to the development of common law are binding in Bermuda. Decisions of the English Court of Appeal and House of Lords are normally highly persuasive and reasoned decisions from commonwealth countries can also be considered.

Civil legislation and common law

The laws of Bermuda allow victims of fraud to avail themselves to many of the same rights and remedies that exist in England and Wales. Remedies such as restitution, damages and/or equitable compensation can be sought from wrongdoers under various types of claims including fraud, unjust enrichment, knowing receipt, breach of contract, misrepresentation, deceit, dishonest assistance, breach of fiduciary duty, and/or breach of trust. Most breach of contract and tort claims have a limitation period of six years.

Criminal legislation

There are various sources of legislation in Bermuda that create statutory criminal offences related to fraud. The Proceeds of Crime Act 1997 (the "**Proceeds of Crime Act**") and the Proceeds of Crime (Designated Countries and Territories) Order 1998 set out money laundering offences and make provision for powers of the Bermuda Court to order confiscation of assets of offenders that are derived from criminal conduct. The Companies Act 1981 (the "**Companies Act**") sets out a range of criminal offences that may be committed by directors of companies, including, for example, by fraudulently altering documents relating to company property or affairs, falsifying books or accounts with the intention of defrauding any person, or fraudulently inducing a person to give credit to the company. Other legislation setting out criminal offences relating to fraud include: Criminal Code Act 1907 ("**Criminal Code**"), Banks and Deposit Companies Act 1999, Bribery Act 2016, Investment Business Act 2003, Investment Funds Act 2006, and the Tax Management Act 1976.

Main stages of fraud, asset tracing and recovery cases in Bermuda

No two fraud, asset tracing, or recovery cases are the same. Accordingly, the stages that may be employed in Bermuda (and abroad) will be driven by a strategy that is best suited to the particular factual landscape and based on a practical understanding of legal actions available. Certain situations may call for letters rogatory or the use of bilateral treaties, whilst others may call for private civil action or arbitration in a financial dispute. Insolvency mechanisms might also be used when a claimant seeks an order to appoint a provisional liquidator to secure the remaining assets for the benefit of creditors, particularly in cases where fraud or misconduct is alleged.

Recovering assets for the victims of a cross-border fraud is often far more complex than attempting to recover assets for a simple debt judgment. Fraudsters often attempt to obscure the ultimate destination of funds with the assistance of unethical facilitators. For these reasons, when assessing a case and a potential asset recovery strategy, it is of the utmost importance that careful consideration be given in the early stages to selecting the remedies that have the greatest opportunity to bring in recoveries. It is also critical to ensure the "team" includes respected legal professionals that understand their own local jurisdictions and also the nuances of offshore.

Stages which may be encountered include: investigations and intelligence gathering; disclosure remedies; insolvency; interim relief; recovery actions; and enforcement. The stages are not entirely linear and in some cases, the stages will need to run concurrently and/or be revisited while making necessary adjustments along the way.

Investigations and intelligence gathering

Once it has been determined that a fraud has likely occurred, a priority is the identification of assets controlled by the fraudster so that, to the extent possible, interim actions aimed at immobilising the assets can be taken. If the assets

controlled by the fraudster have been squandered or lost, the investigator should consider if there are other viable targets. At the same time, the investigator may need to obtain additional information related to the fraud to determine its full extent and nature. This will be important in evaluating which recovery actions are ultimately taken.

Although often not the focus, intelligence gathering and fact finding should not ignore potentially relevant information that is publicly available. In Bermuda there are a number of useful sources including:

- Corporate documents: Certain corporate documents are available to members of the public through the Registrar of Companies for a fee including the company name, registration number, incorporation dates, certificate of incorporation, memorandum of association, registered office, registered charges that have been filed, winding up notices, share capital increase or reduction notices and prospectus registrations.
- Directors and Officers Registry: The Bermuda government maintains a central directory of persons serving as corporate directors and officers that can be searched for free.
- Shareholder/member information: A Bermuda company is required to produce a copy the register of members containing the names of shareholders of a Bermuda company (as well as the directors and officers register) to a member of the public upon request being made to the registered office of the company.
- Court records: Access to court records should not be overlooked. For cases filed after 1 December 2015, and subject to documents protected by privacy restrictions, members of the public have a right to seek certain documents from the Registrar. In respect of pending cases, requests can be made for orders filed in the case, for originating process (e.g. writ, petition, summons), or documents referred to in any public judgment or hearing may be requested. Further requests can be made for documents when the case is no longer pending including for copies of transcripts.
- Shipping and aviation records: Shipping and aviation registers are capable of being searched and copies taken. Details available include registered owner and mortgages filed.
- PATI Requests: Pursuant to the Public Access to Information Act 2010, Bermudians and residents of Bermuda have rights to access records held by public authorities regarding the work they carry out, how and why they make decisions, and how public money is spent. Each public authority must publish an "information statement". If a document is not presently available, a request can be made for its disclosure subject to certain exceptions. Exceptions include when it is in the public interest or for the protection of the rights of others (such as records that deal with personal information), confidential matters such as national security, commercial information or ministerial responsibilities.

Disclosure Remedies

The typical disclosure options available in Bermuda are similar to those available in England and Wales. Two primary options include Norwich Pharmacal Orders and Bankers Trust Orders.

Norwich Phamacal Orders

A Norwich Pharmacal order is typically pre-action and granted against a third party that has been innocently mixed up in wrongdoing, to compel disclosure of documents or information, which may identify another person (for example, a wrongdoer or a potential beneficiary), or to identify the nature of the wrongdoing, both of which may be the subject of subsequent legal proceedings.

To the extent the disclosure identifies additional wrongdoing by the third party, it may be possible to use those documents but that cannot be the purpose for which they were sought. Moreover, one can, where appropriate, apply for a gagging order, which directs the party not to disclose that they have been ordered to provide information to a third party. This is particularly helpful where the respondent is a bank or a professional who may have duties to give notice to their clients of such matters. However, as in England and Wales, in order to obtain a Norwich Pharmacal order, applicants will need to show:

- that there is a 'good arguable case' that a wrongdoing has occurred;
- that the person against whom the disclosure request is sought is involved, albeit possibly innocently, in the wrongdoing as more than a mere witness;
- that the respondent is likely to have the information sought (i.e., it is not a fishing expedition); and
- that the order must be necessary and proportionate, and in the overall interests of justice.

In the context of frauds involving offshore companies, registered agents may well be targets of these types of orders as they have AML/ATF obligations to keep records of beneficial owners.

Such orders normally require that the claimant give an undertaking in damages and to pay expenses resulting from the disclosure sought.

Bankers Trust Orders

Following the principles established in *Bankers Trust v Shapira (1980) 1 WLR 1274*, orders can be sought to compel banks to provide records enabling the assets belonging to the claimant to be traced. Unlike a Norwich Pharmacal order, there is no need to show any involvement in the wrongdoing but a *prima facie* case of fraud or breach of trust needs to be demonstrated. Although there are only four deposit taking banks in Bermuda at present, the reach of these orders has been extended beyond banks to include a defendant against whom a fraud has been alleged.

Similar to Norwich Pharmacal orders, it would be expected that the claimant give an undertaking in damages and to pay expenses resulting from the disclosure sought.

Insolvency

Sometimes a corporate vehicle may have been a central facility used in perpetrating wrongdoing and/or rendered insolvent following a fraud. In these cases, parties should consider whether the use of insolvency proceedings would be advantageous. Whilst perhaps not foremost in the minds of many, it is a tried and tested method, and can be appropriate for both insolvent and solvent companies.

Routes to a court-supervised insolvency would include an application by the directors of the company or it may be that creditors can make valid statutory demands followed by an application to force a compulsory winding-up. In other cases, where there is a *prima facie* case of fraud carried out by the company, victims may be able to make an *ex parte* application (particularly where there is a risk of dissipation or misuse of the company's assets) to compel the appointment of a liquidator on a "just and equitable basis". In such cases, provisional liquidators' powers can be tailored to fit the circumstances.

If winding up order is made, a liquidator will be tasked with realising the company's assets, including commencing potential recovery actions, for the benefit of its stakeholders. Typically, a committee of creditors and/or shareholders can be used by the liquidator as a sounding board regarding the development of a recovery strategy. The liquidator will also have a duty to regularly report to the creditors and shareholders, providing further transparency about the progress of the investigations and recoveries. Where a common interest can be identified, it may be possible for the liquidator and the victims of the fraud to coordinate their investigations and recovery actions.

Insolvency proceedings also provide other valuable advantages including broad rights to collect records and to pursue certain types of claims.

Documents and information available to a liquidator

Liquidators typically have wide powers to request and receive information and documents related to the affairs of the company and can seek orders from the Bermuda Court that relevant persons be summoned or required to respond to written interrogatories. Documents capable of being collected by a liquidator would include the company's banking records, accounting records, historical correspondence, and audit working papers. Directors will also

be under an obligation to prepare a statement of affairs together with a list of creditors and their quantum.

Remedies and claims that can be pursued in an insolvency

Certain types of remedies and claims only arise in an insolvency context, including:

- Fraudulent preferences: Dispositions of property within six months of the commencement of a winding-up are void where (1) it was made with the intention to fraudulently prefer one or more of the company's creditors, and (2) at the time the company was unable to pay its debts as they fell due.
- Avoidance of floating charges: A floating charge will be invalid if it was created within one year of the commencement of the winding up, unless the company was solvent at the time it was created. An exception is made when the charge is made in exchange for cash consideration (plus interest accrued).
- Fraudulent trading: Fraudulent trading is construed as any business carried on by the company with the intent to defraud creditors or for any fraudulent purpose. In these circumstances, a liquidator, creditor, or shareholder may seek that the Bermuda Court make orders that any persons (including directors) who were knowingly parties to the fraudulent trading be made personally liable for all or any of the debts owed by the company.

Parties may wish to consider recent developments in the area of the law following the JCPC decision in *Skandinavska Enskilda Banken AB v Conway and another (as Joint Official Liquidators of Weavering Macro Fixed Income Fund Limited) [2019] UKPC 36*, where it was held (albeit in a Cayman Islands appeal) that a "dominant intention to prefer" could be inferred in certain circumstances where it was well known that payments to one creditor would mean other creditors could not be paid.

Interim relief

Interim relief to prevent the dissipation of assets by, and to obtain information from, those suspected of involvement in the fraud are available in Bermuda including orders for injunction, preservation of property, sale of perishable property and recovery of property subject to a lien.

Freezing injunction (Mareva)

Freezing injunctions can be sought against assets of a party to prevent dissipation pending further order or a final resolution. If a respondent seeks to move or transfer assets without approval, it may be possible to have a contempt order made.

In determining whether and what orders to make, the Bermuda Court has had regard for the authority set down in *Mareva Compania Naviera S.A. v International Bulkcarriers S.A. [1975] 2 Lloyd's Rep. 509, C.A.* Accordingly, a *prima facie* case should be set out for making the orders sought. The party applying for the order will normally need to provide a cross-undertaking to address potential damages and may need to support the same with security.

Search and Seizure (Anton Piller)

Orders for the search of premises and seizure of evidence that is the subject matter of the dispute can be made without warning to the defendant. Such orders can prevent destruction of relevant evidence, and may be particularly useful in ensuring electronic evidence on computers or mobile devices is preserved.

In determining whether and what orders to make, the Bermuda Court has had regard for the authority set down in *Anton Piller v Manufacturing Processes Ltd [1976] 2 WLR*. Accordingly, it would be necessary to demonstrate:

- that there is *prima facie* evidence of the wrongdoing;
- that the potential or actual damage is very serious;
- that there is clear evidence that the respondent has incriminating evidence in his or her possession; and
- that there is a real possibility the respondent may destroy this material if he or she were to become aware of the application.

Recovery actions

The typical actions considered by civil plaintiffs in Bermuda are, as mentioned earlier, similar to those that exist in England and Wales. Avoidance type actions are also commonly considered, including:

- Fraudulent conveyances: The Bermuda Conveyancing Act 1983 contains statutory provisions allowing for dispositions of property to be set aside where they were carried out at undervalue and coupled with a dominant intention of putting property beyond the reach of creditors. The terms "disposition" and "property" are widely defined and interpreted so that their use can be applied to a variety of situations.
- Undisclosed conflicts of interest: Conflicts of interest by a director which are not disclosed in relation to contracts entered into by a company and a third party may result in the avoidance of the contract (and recovery of profits) at the instance of the company. Such non-disclosure can also result in the relevant

director being deemed to not to be acting honestly and in good faith.

Claims are normally commenced by issuance of a generally or specially indorsed writ. Issuance of a writ can be done for protective purposes; however, typically they must be served within a period of 12 months. If defendants are located abroad, permission to serve must be sought in advance. Once served, the defendant must enter an appearance failing which a judgment in default of appearance may be sought. Unless the writ is specially indorsed, the plaintiff will be required to serve a statement of claim followed by the defendant's defence.

Following pleadings, the parties must enter into discovery by exchanging a list of documents under their custody, power, or possession and allowing for their inspection. The Bermuda Court will make directions regarding case management and time-table matters such as discovery, interrogatories, witness statements, and expert reports. Strike out and summary judgment orders can be sought throughout the process.

Surviving claims are typically able to reach trial within 18 months from commencement. Hearings are generally matters which are open to the public, but may be held behind closed doors if there is a risk that privileged or confidential information may be disclosed.

Enforcement

There are a variety of options to pursue enforcement in Bermuda. Money judgments create a lien over real property situated in Bermuda that is registered in the judgment debtor's name. A writ of execution against a judgment debtor's assets can be effected through seizure and sale of the assets, or orders made for garnishment or appointment of a receiver. If enforcement requires a defendant to take or refrain from taking some action, it may be possible to obtain orders for sequestration or committal.

The Proceeds of Crime Act provides for the confiscation of assets upon application by the Department of Public Prosecutions or by the Bermuda Court of its motion. Where a victim's assets have been recovered pursuant to a recovery order under the Proceeds of Crime Act, an application can be made to the Bermuda Court for an order declaring the assets as belonging to the victim.

Reporting

Parties involved in a fraud investigation should be mindful of their anti-money laundering obligations under the Proceeds of Crime Act to report suspicious activity to the Financial Intelligence

Agency when their investigations give rise to a suspicion that assets are the proceeds of crime and/or money laundering offences which have or are taking place.

Parallel proceedings: a combined civil and criminal approach

It is possible to advance civil proceedings that are based on the same set of facts as an overlapping criminal complaint; however, the Bermuda Court has discretion to stay the civil proceedings. In determining whether civil proceedings should be stayed, the Bermuda Court has weighed the competing considerations of the parties and considered whether continuation of civil proceedings runs a real risk that the defendant's fair criminal trial rights would be prejudiced. The burden for demonstrating this prejudice lies with the defendant. This issue was recently dealt with in the matter of *Hiscox Services Ltd et al. v Y Abraham [2018] SC (Bda) 68 Civ (5 October 2018)* where the Bermuda Court relied heavily the JCPC decision in *Panton v Financial Institutions Services Ltd [2003]*. In the Hiscox matter, the defendant did not file any evidence in relation to a summary judgment application. In the circumstances, the Bermuda Court found that a summary judgment did not present a real risk that the defendant's fair criminal trial rights would be prejudiced.

Key challenges

Funding and Costs

A challenge for victims of fraud are the ever-increasing costs of funding the investigations

and claims, particularly for victims who have lost significant, and life changing sums. While lawyers are prohibited in general from operating on conditional or contingency fee arrangement, third-party funding has been embraced. In the matter of *Stiftung Salle Modulable and Rütli Stiftung v Butterfield Trust (Bda) Ltd [2014] Bda LR 13*, a third-party funding arrangement was alleged to be champertous and unlawful. However, in its ruling, the Bermuda Court found that such arrangements were valid, supported constitutionally protected rights of access to the court, and should be encouraged. Funders should, of course, exercise professional judgment and caution as third-party cost awards are possible in Bermuda and have been made against funders in the past as was done in *Majuro Investment v Vasile Timis et al [2016] SC (Bda) 22 Com (10 March 2016).*

Reputation

Historical misconceptions and reputational issues concerning offshore jurisdictions can have real world negative impacts that hinder investigations and asset recovery efforts, including when seeking assistance from foreign courts. On at least one occasion, a European authority has rejected a request for assistance from a Bermuda litigant citing reasons including, among others, that the international cooperation would constitute an insurmountable obstacle that would delay proceedings.

Despite the concerns of certain jurisdictions, other independent organisations tasked with assessing the level of international cooperation have in fact praised Bermuda. On 17 January 2020, the Caribbean Financial Action Task Force made public the results of a mutual evaluation report of Bermuda's systems and framework to combat money laundering and the financing of terrorism and proliferation. These results placed Bermuda in the highest technical compliance out of 75 countries evaluated to date and cited a substantive overall effectiveness of Bermuda's AML and ATF regime including, in the category of "international cooperation activities to provide intelligence and evidence to facilitate action against criminals".

Cross-jurisdictional mechanisms: issues and solutions in recent times

As noted, most fraud, asset tracing and recovery matters touching Bermuda involve parties located outside of the jurisdiction. Consequently, it is not uncommon for there to be foreign litigants that seek assistance from a Bermuda Court and/or for a Bermuda litigant to seek assistance of foreign courts.

Seeking Assistance from Foreign Courts:

Depending on which foreign jurisdiction a Bermuda litigant is seeking assistance from, there are various methods or approaches for requesting international assistance, including: seeking to have Bermuda judgments recognised and enforced abroad; for freezing orders in aid of Bermuda proceedings; or to seek evidence located abroad. Letters rogatory may be needed to request these types of assistance.

Some jurisdictions, such as the United States, allow foreign litigants access to disclosure without the need for letters rogatory. This is highlighted not because it is a Bermuda-specific remedy, but because so many international fraud cases, including those in Bermuda, involve the movement of United States' dollars which necessarily pass through its correspondent banks, many of which are located in New York. As such, records of these transfers can be subpoenaed under section 1782 of title 28 of the US Code so long as the claimant meets the definition of "interested person" and the information sought is for use in a foreign or international tribunal. United States courts have interpreted these provisions broadly so that the foreign proceedings in which the documents might be used do not even need to be pending and may be sufficient that they are merely contemplated. Needless to say, this is a tool used by Bermuda litigants to good effect in fraud and asset tracing cases including recently in *Hiscox Services Ltd. et al v. Montres Journe New York LLC.*

Bermuda liquidators can also seek formal recognition of their appointments and powers by foreign courts enabling them to control assets,

collect additional evidence, and/or commence litigation abroad. In these circumstances, it will often assist the liquidator when the order appointing him or her specifies that they are empowered to seek such recognition and take such actions in a particular jurisdiction.

Assistance that can be obtained from Bermuda Court:

Taking of Evidence

A letters rogatory type process is available under the Bermuda Evidence Act 1905. An *ex parte* application is made seeking the assistance of the Bermuda Court to which the letters of request issued by the foreign court are appended. This process can be used to compel a person to be examined under oath and/or for production of certain documents.

Assistance to Foreign Insolvencies

There is no statutory provision providing for the recognition of foreign insolvency proceedings or their representatives in Bermuda. However, the JCPC held in a Bermuda matter that there is a common law power to assist a foreign winding up so far as the Bermuda Court properly can under established Bermuda legislation, public policy, and within its own statutory and common law powers. This concept of modified universalism was enshrined in the landmark case *Singularis Holdings Limited v PricewaterhouseCoopers [2014] UKPC 36* but also illustrated the limits of such assistance. In the Singularis case, the foreign liquidators failed to obtain the assistance sought (disclosure from the company's auditors) on the basis that this was not relief that they enjoyed under their own domestic legislation.

Service of Foreign Proceedings

Bermuda is obliged to assist in the service of foreign process on local defendants pursuant to The Hague Convention on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters which has been extended to Bermuda through the United Kingdom.

Injunctions

When the Bermuda Court has jurisdiction over a defendant, interim orders for injunctive relief can be granted in support of foreign proceedings. In such cases, it is necessary to make out a good arguable case for the relief sought in the foreign jurisdiction. In considering whether it is just and convenient to grant an injunction, the Bermuda Court has considered, among other things, whether there is evidence that the foreign court would construe such relief as judicial assistance. These issues were considered by the Bermuda Court in the matter of *ERG Resources LLC v Nabors Global Holdings II Limited [2012] Bda LR 30*.

Enforcement of Foreign Judgment

It is possible to enforce final foreign money judgments in Bermuda under the Judgments (Reciprocal Enforcement) Act 1958 when they emanate from the following British commonwealth countries: United Kingdom; Australia (including most territories and possessions); Hong Kong; Gibraltar; Jamaica; Barbados; Grenada; Guiana; the Leeward Islands; St. Vincent; Dominica; St. Lucia; and Nigeria. Notably absent from this list are the United States, Canada, and most countries of the European Union.

Alternatively, enforcement of a money judgment can take place at common law by commencing proceedings in the Bermuda Court and applying for summary judgment.

Enforcement of Foreign Arbitration Awards

Foreign arbitration awards made in another contracting state can be enforced pursuant to the New York Convention 1958 and the Bermuda International Conciliation and Arbitration Act 1993. The Bermuda Court has demonstrated a pro-enforcement stance and can make orders in support of non-final arbitration awards. This was demonstrated recently, in the case of *CAT. SA v Priosma Limited [2019] SC (Bda) 56 Com*

(3 September 2019), where the Bermuda Court ordered a stay of enforcement proceedings before it pending the outcome of a final appeal but only on the condition that the defendant provide full security in the amount of the award and costs.

Court to Court Communications

During March 2017, the Bermuda Court became the first court from offshore jurisdictions to issue a new practice direction adopting the Judicial Insolvency Network Guidelines for Communication and Cooperation between Courts in Cross-Border Insolvency Matters.

Technological advancements and their influence on fraud, asset tracing and recovery

Blockchain and Digital Asset Technology

The government of Bermuda has made no secret that it is committed to working with the fintech industry in seeking to establish Bermuda as a world leader in this space and to add it as a new economic pillar. To that end, Bermuda has passed several key legislative acts including the Virtual Currencies Business Act 2018, the Digital Asset Business Act (DABA) 2018 ("**DAB Act**"), and The Companies and Limited Liability Company (Initial Coin Offering) Amendment Act 2018. The acts identify certain categories of activities that are subject to gatekeeping approval processes for new entrants, establishes a framework for operation, and mandates regulation of those engaged in the digital asset business. These laws also create a broad range of new offences which carry steep fines and the potential for imprisonment for offenders.

In keeping with its traditional approach of quality, Bermuda appears to be taking a cautious approach in approving new entrants to operate under the relevant legislation. One aim of the fintech revolution is to increase audibility of transactions which in theory should enhance ability to "trace" assets. Nevertheless, the technology and laws in the virtual currency space are rapidly evolving and, likewise, fraudsters will adapt quickly in seeking to exploit these industries to steal, hide and/or move assets.

Bermuda's legislation does contain aspects that will guard against offenders and assist future asset recovery professionals. For instance, the DAB Act contains requirements that licensed undertakings must maintain a record of both its client and its own transactions at its head office, which must be located in Bermuda. In addition, licensed undertakings that hold client assets, will need to provide security in the form of surety bond, trust account, or indemnity insurance in such form and amount as acceptable to the Bermuda Monetary Authority.

Judicial Technology

The Bermuda Court is expecting to enhance its technological capability through the Evidence (Audio Visual Link) Act 2018. Although not yet in force, the act will allow evidence to be taken remotely from vulnerable witnesses and/or overseas witnesses and experts. It should also be noted that the Bermuda Court has previously exercised its discretion in favour of receiving evidence remotely in circumstances where no real contention arose between the parties in so doing.

Recent developments and other impacting factors

Economic Substance

Bermuda, like many other major offshore financial centers, has adopted economic substance legislation that will change the landscape for many traditionally so-called "letter box" companies. The Economic Substance Act 2018 (as amended) requires companies engaged in relevant activities to provide evidence of economic substance in Bermuda including: being managed or directed; having adequate and suitably qualified employees; having adequate expenditure, having adequate physical presence; and in conducting core income generating activities.

The impact of this legislation is still cascading through Bermuda's marketplace, but one should expect that local service providers in Bermuda will play an increasingly important role in assisting many Bermuda-domiciled companies to meet their economic substance requirements. Further, the increased activities and presence of these companies means that there will likely be a corresponding increase in information and/or assets located in the jurisdiction, which in turn will be of interest and value to future asset tracing and recovery exercises.

Beneficial Ownership Registers

The Bermuda Monetary Authority maintains a private central beneficial ownership registry of Bermuda companies and partnerships (excluding certain exempted categories) for which information is collected, including: full name; residential address; nationality; date of birth; and nature and extent of interest in the company or partnership. Despite plans by the UK and EU to implement public beneficial ownership registers and pressure on Bermuda to do the same, there has been no firm commitment by the government to do so. During October 2019, a spokesperson for the Bermuda government is reported to have said "we are committed to implementing any properly adopted international standard for public registers and will continue to work with bodies like the Organisation for Economic Co-operation & Development and the Financial Action Task Force to combat money laundering".

Mathew Clingerman is the managing director of KRyS Global in Bermuda and has oversight of its forensic technology services. He has over 15 years of professional experience involving cross-border asset recovery investigations and insolvencies. He has acted as an independent expert, court-appointed liquidator, court-appointed receiver, and is a recommended expert by *Who's Who Legal 2019* in the area of restructuring and insolvency advisors. He holds a Bachelor of Science degree in Accounting and is a Fellow of INSOL International, a Chartered Financial Analyst, and a Certified Fraud Examiner. He sits on the Committee for the Restructuring and Insolvency Specialists Association in Bermuda.

mathew.clingerman@krys-global.com

British Virgin Islands

Jonathan Addo
Harneys

John McCarroll SC
Harneys

Christopher Pease
Harneys

Stuart Rau
Harneys

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

In cases of fraud, asset tracing and recovery, the BVI courts and the litigants who bring their cases before them have at their disposal a wide range of remedies that will be familiar to fraud practitioners in common law jurisdictions. These remedies have their roots in both legislation and in the body of case law arising from both common law and equity. The common law of England was introduced by the Common Law (Declaration of Application) Act 1705 and the rules of equity by Eastern Caribbean States Supreme Court (Virgin Islands) Act 1969.

Injunctive relief

The most common disputes arising in this field concern the beneficial ownership of shares in BVI registered companies and proprietary injunctions are accordingly frequent. The statutory root of the court's jurisdiction to grant injunctive relief (and to appoint a receiver on an interlocutory basis) arises from Section 24 of Eastern Caribbean Supreme Court (Virgin Islands) Act 1969 (Cap 80), which provides that the court may make such an order:

> "*…in all cases in which it appears…to be just or convenient and any such order may be made either unconditionally or upon such terms and conditions as the court or judge thinks just.*"

This section for the basis of all injunctive relief including the granting of freezing orders (see for example *Danone Asia PTE Limited v. Golden Dynasty Enterprise Limited* (BVIHCV 2007/0262)).

The High Court also has inherent jurisdiction under which orders and ancillary orders may be granted. See section 7 of ECSCC 1969.

Approach to injunctions

In determining whether injunctive relief should be granted, the court applies the guidelines set out in *American Cyanamid v. Ethicon Limited [1975] AC 396* and English (and other Commonwealth) authorities have been relied upon with regard to various elements of the guidelines (for example, the test for good arguable case contained in *Ninemia Maritime Corp v. Schiffahrtgesellschaft gmBH & Co KG (The Niedersachsen) [1984] 1 All ER 393*).

Orders which are ancillary to the granting of injunctive relief, such as interim disclosure orders in aid of proprietary or freezing injunctions, are commonly made where required.

As a general note, although the BVI has a growing body of case law of its own (to which the doctrine of precedent applies), it is relatively small in terms of volume. Whilst the common law of England has been carried into BVI law by statute, English authorities do not bind the BVI courts. They are, together with decisions from other common law jurisdictions, persuasive and are frequently cited. While the BVI is part of the Eastern Caribbean Supreme Court (and appeals are made to the Eastern Caribbean Court of Appeal), decisions from other member states are not binding on the BVI courts.

The Eastern Caribbean Supreme Court Civil Procedure Rules (ECC PR) also make specific procedural provision with regard to injunctive and other interim relief (CPR rule 17). Most notably in this regard EC CPR Part 17.4(4) provides that the court has power to grant an interim order made without notice for a maximum period of 28 days. This requires the return date to be listed within that time period. Notwithstanding the fixing of the return date, an applicant must file a formal application to continue the relief. Otherwise interim applications must be made with at least three days' notice to the Respondent.

Stop Notices

EC CPR Part 49 contains the basis for applying for Stop Notices in respect of shares. A Stop Notice may be served by any party who claims to be beneficially entitled to the shares and requires the party on whom it is served to refrain from taking any "specified steps" without first notifying the person on behalf of whom the notice was served. "Specified steps" include the transfer, sale or registration of shares and the making of any payment by way of dividend or otherwise in respect of the shares. The procedure is designed to be simple with the Notice issued by the court office on filing the appropriate form and a supporting affidavit. The Notice does not, however, prevent dealing in the shares, merely that the recipient gives notice of his intention to take any specified steps before doing so. The court also has power to issue a Stop Order (EC CPR 49.7) to prohibit the taking of specified steps. While Stop Notices are commonly issued at the early stage in order to give a modicum of protection with regard to disputed shares and sometimes to flush out the intentions of the registered owner, in disputed cases Stop Orders are rarely sought as parties prefer instead to seek injunctive relief.

Receivers

BVI courts can and do appoint receivers over assets to preserve them pending trial. The statutory basis is contained, in common with injunctions in section 24 Eastern Caribbean Supreme Court (Virgin Islands) Act 1969. These are distinct from receivers appointed post-judgment.

Norwich Pharmacal and search orders

Norwich Pharmacal orders are amongst the most common orders made in the BVI by reason (and are dealt with in a different chapter). There is no statutory basis for such orders and the jurisdiction is based on the eponymous English case *Norwich Pharmacal Co v. Customs and Excise Commissioners [1974] AC 133*, which has been followed and applied in numerous BVI authorities. Similarly,

search orders have no statutory basis (although procedural provision is made for them in EC CPR Part 17). Such orders, as elsewhere, are comparatively rare.

Asset tracing

The BVI recognises a number of causes of action in this regard, including dishonest assistance, bribery, secret commissions and knowing receipt. None of these are based on statute.

Enforcement and relief in aid of foreign proceedings

Prior to 2010, freezing injunctions were only available in relation to a substantive domestic claim. However in *Black Swan Investment ISA v. Harvest View Limited BVIHCV (COM) 2009/0399* the Commercial Court held that it had discretion to grant a standalone freezing injunction in support of foreign proceedings (including arbitrations) in cases where the defendant was within the *in personam* jurisdiction of the BVI courts. This advance was confirmed by the EC Court of Appeal in *Yukos Cis Investments Limited v. Yokos Hydrocarbons Investments Limited HCVAP 2010 0028*. While the underlying basis for freezing orders is contained in statute (see above), this now well-established refinement is purely a creature of case law. In order to obtain what is now commonly known as a "Black Swan Order" the following must apply in addition to the normal requirements in respect of freezing orders:

(1) It must be made in aid of relief the applicant is likely to obtain from the foreign court.
(2) If the relief sought goes beyond the scope of the foreign proceedings, the court will not normally make the order.
(3) The relief sought must lead or be likely to lead to a judgment capable of being enforced in the BVI.
(4) The failure to seek injunctive relief in the foreign proceedings is a discretionary factor which militates against relief being granted.
(5) In addition to having *in personam* jurisdiction over the respondent, the court must also have jurisdiction over the assets sought to be frozen.

With regard to enforcement generally, EC CPR makes provision for the enforcement of judgments both domestic and foreign together with arbitral awards. These include the normal tools of enforcement found throughout the common law world including charging orders, garnishee orders, judgment summons, orders for the seizure and sale of goods and the appointment of a receiver. Further, Part 46 provides for writs of execution including orders for the sale of land, seizure and sale of goods, sequestration of assets and writs of delivery and possession.

Insolvency regime

As a great deal of BVI litigation is company-related, the insolvency regime, as contained in the Insolvency Act 2003, is of particular importance. Liquidators are given powers to set aside transactions made while the subject company was insolvent (during a defined vulnerability period) and which have improperly diminished the assets which would otherwise have been available for creditors. There are four types of voidable transactions: unfair preferences; transactions at an undervalue; voidable floating charges; and extortionate credit transactions. Further, Part IX of the Act deals with the liquidator's powers to take action against those who have been guilty of misfeasance, insolvent trading and fraudulent trading.

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

Where a fraud is suspected, the first stage for a victim will ordinarily be to learn as much as possible about what has happened. However, the victim needs to carry out an initial investigation as quickly as possible and without alerting any of the suspected wrongdoers to the fact that the fraud has been uncovered. In practice the

investigation phase will therefore often coincide with the victim seeking interim relief from the court.

In the BVI there is no procedural jurisdiction to grant pre-action disclosure. As a result, a practice has grown in obtaining this form of disclosure through the common law route developed in England through the principles established in the Norwich Pharmacal and Banker's Trust cases (Norwich Pharmacal Orders), named after the eponymous English appellate cases of *Norwich Pharmacal Co. & Others v Customs and Excise Commissioners* [1974] AC 133 and *Bankers Trust v Shapira* [1980]1 WLR 1274.

These types of orders are frequently sought to reveal key pieces of information that will enable the victim to bring a claim against the wrongdoers and/or to take protective measures (*Rugby Football Union v Consolidated Information Services Ltd* [2012] UKSC 55; *UVW v XYZ* (BVIHC (COM) 108 of 2016)). Such orders are commonly sought against BVI registered agents in order to obtain information relating to the management and ownership of BVI companies, which makes them a particularly useful tool where BVI companies have been used as part of a fraud Evidence in support of a Norwich Pharmacal Order can often be complemented by evidence obtained. All companies registered in the BVI must be administered by a registered agent located in the BVI and the courts have, as a general rule, found that where a BVI company has engaged in wrongdoing or otherwise become mixed up in wrongdoing, the registered agent will also have become mixed up in the wrongdoing (albeit innocently) (*JSC BTA Bank v Fidelity Corporate Services Limited* (HCVAP 2010/035)).

Given that registered agents are required by law to retain know-your-customer (KYC) documentation showing the ultimate beneficial owner of the companies they administer, a successful Norwich Pharmacal application would reveal the ultimate beneficial owner of a BVI company and, for example, confirm that payments made to that company were in fact for that individual's ultimate benefit.

They might also be used to determine the suspected wrongdoer's connections with third parties, whether he or she has interests in other companies registered in the BVI and reveal whether the wrongdoer and his companies own certain assets. By contrast to the English position, Norwich Pharmacal Orders may be obtained against entities in the BVI for the disclosure of information that will be used in support of substantive proceedings elsewhere (*The President of the State of Equatorial Guinea v Royal Bank of Scotland International* [2006] UKPC 7; *Q v R* (unreported, 13 December 2018); *BBB (A fund acting by its investment manager) & Another v UUU Ltd (a registered agent)* BVIHC (COM) 0182 of 2019). Crucially, Norwich Pharmacal Orders are ordinarily preceded by protective seal and gag orders that prevent tipping off by the respondent party (often a registered agent of a BVI company) (*Banco Ambrosiano Andino S.A. v Banque Nationale de Paris* [1985] HKLR 72).

Once a victim knows the identity of the wrongdoer(s) and has evidence that they have assets which are at risk of dissipation, the victim will often apply for a freezing injunction in order to prevent the wrongdoer disposing of their assets. In the BVI, such orders are frequently obtained directly against the BVI companies that are owned by the ultimate wrongdoer in order to prevent those companies from disposing of any assets up to the value of the wrongdoers suspected liability (which will usually correlate with the extent of the victim's loss). Such relief will be available even if the ultimate wrongdoer is not located in the BVI and if the substantive proceedings, in support of which the injunction is sought, are taking place elsewhere (*Black Swan Investment I.S.A. v Harvest View Limited and Another* BVIHCV 2009/399; *Yukos CIS Investments v Yukos Hydrocarbons Investments Limited* HCVAP 2010/028; *Osetinskaya v Golante and Usilett* BVIHC 2013/0037). Where it is anticipated that substantive proceedings will be commenced in the BVI in relation to the fraud, injunctions might also be sought against the wrongdoers that are not located in the BVI.

With regard to substantive claims, the claims commonly used to combat fraudulent practices in the BVI include: civil bribery; knowing receipt; dishonest assistance; unjust enrichment; conspiracy; and breach of fiduciary duties. Liquidators can also commence statutory claims in relation to fraudulent transactions perpetrated by the directors or officers of a company. Such claims tend to arise out of the payment/receipt of bribes or the dishonest transfer/receipt of monies or assets. Claims will often be brought in the BVI where BVI companies are used as vehicles to receive the tainted monies or assets and where the company is therefore a natural defendant to one of the claims mentioned above. However, in circumstances where many of the actions giving rise to the fraud are known to have taken place elsewhere, and where those involved in the fraud (and who are obvious witnesses to any claims arising out of it) are located elsewhere, such claims may be liable to be stayed in the BVI pending determination of the same or similar causes of action in whatever other jurisdiction is considered to have a closer connection to the

underlying dispute and where the courts of that jurisdiction are therefore considered to be a more appropriate forum to determine the claim.

As explained in more detail below, it is possible that the criminal authorities in the BVI will commence an investigation into cases of suspected fraud and that such an investigation will lead to a public prosecution. However, this is relatively unusual. It is more common in the BVI for instances of fraud to be dealt with by way of civil claims, or for the action to be dealt with in other jurisdictions (depending on where any wrongdoing is found to have taken place).

There are various post-judgment tools that can be used by judgment creditors against judgment debtors located in the BVI or who have assets located in the BVI:

1. where judgments are obtained directly against BVI registered companies and the judgment is unsatisfied, the judgment creditor can apply to wind up the company and appoint liquidators. This is a powerful tool that allows a court-appointed officer access to the company's books and records which may reveal further crucial information regarding the wrongdoing and/or the wrongdoers' assets;
2. where there is evidence that the judgment debtor owns BVI companies, the judgment creditor can apply for charging orders against those companies, which ultimately allows the creditors to appoint a receiver to sell the companies and/or their assets to satisfy the judgment debt; and
3. a judgment debtor can be summoned to appear before the court to give evidence as to his or her assets and risks being in contempt of court if they fail to appear, which could ultimately lead to committal proceedings.

Contrary to popular belief, the BVI legal system mirrors the English legal system in many respects and has established jurisprudence that is favourable to victims and creditors. In effect, genuine victims of fraud are, if their case meets the relevant threshold requirements, able to control how they investigate and prosecute suspected frauds, which means they can make confidential applications for further information and for protective relief before the suspected wrongdoers are made aware that legal proceedings have been commenced. The insolvency framework means that obtaining judgments against BVI companies can yield further information, in addition to locating assets owned by those companies.

Parallel proceedings: a combined civil and criminal approach

Whilst it is possible to commence parallel criminal and civil proceedings in the BVI, in practice it is uncommon for the criminal authorities in the BVI to pursue wrongdoers that are located abroad.

A victim of fraud is able to initiate criminal proceedings by lodging a complaint with the Magistrate's Court. Once a complaint has been lodged, the Magistrate will make a determination on whether or not to issue a summons directing that the person against whom allegations are made in a complaint should appear before the Magistrate's Court to answer the charge or complaint made against them. Should a summons be issued, it means that matters will proceed to an initial hearing and the time and date for that first hearing will be given by the

Magistrate upon issuing the summons. The main point the court will consider when determining whether or not to issue the summons is whether the allegation is known to the law and whether the ingredients of the offence are, *prima facie*, present.

In cases where the complaint gives rise to criminal proceedings, the Magistrate's Court will ordinarily inform the DPP or the AG of the complaint. The DPP and the AG would then have a discretion as to whether to take over the prosecution. However, in the event that they choose not to bring a public prosecution, there is no restriction on a private person bringing such prosecution.

One of the advantages of commencing criminal proceedings will often be the investigative powers available to the authorities, not only within the jurisdiction where the proceedings are ongoing, but to request assistance from authorities overseas. However, it does not allow a private entity that is prosecuting criminal proceedings to make an application for assistance from authorities overseas.

In addition, or alternatively, a victim may submit a suspicious activity report (SAR) in instances where they consider that a BVI entity has dealt with or possesses property comprising the proceeds of crime. Once a SAR has been submitted, the FIA will consider it and determine whether to commence an investigation. The FIA is responsible for receiving, obtaining, investigating, analysing and disseminating information which relates or may relate to a financial offence or the proceeds of a financial offence; or a request for legal assistance from an authority in a foreign jurisdiction which appears to the FIA to have the function of making such requests.

One potential risk of commencing parallel proceedings is that a defendant subject to two sets of proceedings may seek to argue that the civil proceedings should be stayed pending determination of the criminal proceedings. The civil courts in the BVI have a general discretion to stay proceedings. Where there are parallel criminal and civil proceedings afoot, the court will stay the civil proceedings if it is satisfied that there is a real risk of serious prejudice to the defendant(s) which may lead to injustice (*R v. Panel on Takeovers and Mergers, ex parte Fayed* [1992] BCC 524). When determining whether there is a real risk, the court will take into account the interests of justice and the positions of the parties (*Panton and others v. Financial Institutions Services Ltd* [2003] UKPC 95).

Generally speaking, it will be difficult for a defendant to persuade a court that there is a real risk of serious prejudice simply because it has to defend civil and criminal proceedings at the same time and the court will not consider an obligation to serve a defence in civil proceedings before they are required to take any similar steps in criminal proceedings. Nor is it enough that both the civil and criminal proceedings arise from the same facts, or that the defendant has to take steps such as serving witness statements and disclosing document within the civil proceedings (*FSA v. Anderson* [2010] EWHC 308 (Ch)).

Should the defendant be able to demonstrate that there is a real risk of serious prejudice leading to injustice if the civil proceedings continue, the court may still refuse to stay the civil proceedings if it can be satisfied that sufficient safeguards are put in place to protect against the risk of injustice.

Cross-jurisdictional mechanisms: issues and solutions in recent times

Pre-action disclosure

Norwich Pharmacal relief is a common route to obtaining pre-action disclosure in the BVI, given the absence of a statutory equivalent in the BVI procedural rules. The courts typically allow *Norwich Pharmacal* relief in support of foreign proceedings provided the disclosure defendant is subject to the jurisdiction, although the court has left room for debate on the issue (*Q v R Corp,* unreported, 13 December 2018).

Disclosure is also available as ancillary relief to a freezing order, although this is not currently available in respect of a freezing order made in support of foreign proceedings where the cause of action defendant is outside of the BVI (*Bascunan v. Elsaca* BVIHC (Com) 2015/0128).

Such relief is, however, available where the freezing order is made in support of arbitral proceedings, provided the foreign arbitral award, when granted, can be enforced in the BVI (there does not need to be an intention to do so) (Section 43, Arbitration Act 2013; *Koshigi Limited & anor v. Donna Union Foundation* BVIHCMAPP2018/0043 and 0050).

Substantive jurisdiction

The BVI largely follows the test for *forum non conveniens* set out by Lord Goff in *Spiliada Maritime Corp v Cansulex Ltd* [1986] UKHL 10. The Court should determine whether there is another available forum, whether it is more appropriate and, if so, a stay should be granted unless there is a risk of injustice in that forum.

The Court of Appeal recently held that the mere involvement in the proceedings of a company incorporated in the BVI, and by implication its shareholders' or controllers' choice to use the BVI in its corporate structure, is not a factor in support of grounding jurisdiction (*Livingtson & ors. v JSC MCC Eurochem & anr.* BVIHCMAP 2016/0042-0046). The decision may be considered by the Privy Council in 2020.

Enforcement

Foreign money judgments are enforceable in the BVI under common law. The courts will not typically conduct a review of the merits of the foreign judgment. Pursuant to statute, judgments from a number of Commonwealth countries can also be reciprocally registered and enforced. Judgments for non-money relief are not enforceable under either option.

Recognition of a foreign judgment can be defended if it would violate public policy in the BVI, if the foreign judgment was obtained by fraud or in breach of natural justice, if the foreign court lacked personal jurisdiction over the defendant or the judgment is not final and conclusive. In addition, there is a wider stipulation that it be just and convenient to enforce the foreign judgment.

It is also possible to apply to liquidate a company on the basis of an unpaid foreign judgment.

Technological advancements and their influence on fraud, asset tracing and recovery

Technology is high on the agenda of the profession in the BVI.

The BVI Financial Services Commission recognises a number of cryptocurrency-based funds including those based on Bitcoin and Ether. As a result, there is a burgeoning cryptocurrency funds sector in the BVI, with leading fintech companies such as Football Coin and Bitfinex incorporated in the BVI. The BVI government has also announced its intention to partner with LIFElabs.io, a cryptocurrency management company, to create a cryptocurrency pegged to the US Dollar for use within the jurisdiction. While the status of cryptocurrencies has not been tested in court, we would expect the court to recognise cryptocurrency as property (similar to the Singaporean decision in *B2C2 Ltd v Quoine Pte Ltd* [2019] SGHC(I) 03), thereby opening up pre-existing remedies in law for fraud, asset tracing and recovery remedies.

Further, crypto-assets, while enabling anonymity, typically use blockchain technology and an immutable public transaction ledger, which may assist with tracing transactions.

The BVI has seen a significant focus on data security, particularly following high-profile offshore hacks such as the "Panama Papers". In 2017, the BVI enacted the BVI Ownership Secure Search System Act, facilitating the storage and retrieval of beneficial ownership information for all BVI companies and legal entities. This uses cloud-based technology to facilitate a private search system accessible to law enforcement agencies in the combat against international crime and illicit financial activity.

The BVI legal profession has keenly adopted the use of technology in investigations, including artificial intelligence and data processing tools for large-scale documentary review exercises and forensic accounting programmes.

The BVI has also enacted the Computer Misuse and Cybercrime Act 2014, which sets out offences relating to cybercrime including

unauthorised access to computer material and unlawful publication of computer data. The legislature is also in advanced stages of introducing amendments to include online crimes such as criminal deception amid other offences.

The implementation of the electronic litigation portal has further facilitated and streamlined the process for filing and management of court cases in the jurisdiction of the Eastern Caribbean Supreme Court.

Recent developments and other impacting factors

On 1 January 2019, the BVI Economic Substance (Companies and Limited Partnerships) Act 2018 came into force (the ESA). The draft International Tax Authority Economic Substance Code issued on 22 April 2019 supplements the ESA. The ESA is in response to guidance issued by the EU Code of Conduct Group for Business Taxation on the economic substance of BVI entities and other jurisdictions with low corporate tax rates.

The BVI has passed the ESA as part of its longstanding commitment to international best practice. The ESA contains a number of requirements as to reporting and economic substance for "legal entities" (essentially companies and limited partnerships) conducting "relevant activities", i.e.: banking; insurance; shipping; fund management; financing and leasing; headquarters; distribution and service centres; holding company; and intellectual property. This will be ascertained under reporting periods lasting less than one year. The ESA allows legal entities carrying out relevant activities (except entities whose only activity is to hold equity) to conduct the relevant activity and generate income. This includes demonstrating sufficient employees and expenditure as well as physical premises for that purpose.

In a decision handed down in May 2019, the BVI court decided that it does have the jurisdiction to grant charging orders, based on English statute predating 1940 (*Commercial Bank of Dubai v Abdalla Juma Majid Al-Sari & Ors.* BVIH(COM) 114/2017). Charging orders are an important tool, particularly when enforcing foreign judgments, as they allow creditors to take a proprietary interest over assets owned by a debtor and ultimately can facilitate the sale of such assets in order to allow the creditor to realise their debt. The decision should therefore be welcomed, as it avoids the need for the legislature to step in and fill what would otherwise have been a significant lacuna in BVI law.

Key Challenges

The increasingly global nature of the corporate landscape with larger numbers of jurisdictions involved in structures and transactions presents more opportunities not just for profits but also for fraud. At the same time, the barrier between the cyber world and tangible assets is ever diminishing and the instances of fraud involving online or digital elements is on the rise. The fraudulent arrangements coming to light in proceedings in the BVI are therefore becoming more challenging to detect with current procedures, while also raising difficulties for tracing after the event, with funds moving at unprecedented speed. In addition, competing interests on the global stage are leading to an increasing number of state-sponsored events.

Prosecuting authorities, with greater powers to identify and freeze assets, are often under-resourced and slow to react. The high cost of litigation without guarantees of success can make it a difficult decision for private parties. It is common in the BVI to use nominees, complex international corporate structures, trusts and nominees as shareholders and directors which create legal barriers to the identification and tracing of assets by civil routes. The BVI also sees limited public corporate information published on the companies registry, leaving action against a company's agent in the BVI as the leading option to obtain corporate information. This can be expensive and leaves no guarantee of success since BVI company law allows corporate documents to be held by others outside of the jurisdiction.

Jonathan Addo is a partner in Harneys litigation, restructuring and insolvency group. He specialises in shareholder disputes, commercial fraud; asset tracing and directors duties, advising major corporations and investors on complex commercial litigation. He has particular expertise in complex hedge fund-related litigation.

Prior to joining Harneys in 2012, Jonathan practised as a barrister at the Bar in London and previously worked in the investment management division of Goldman Sachs International between 2004 and 2008.

Jonathan is a leading lawyer in the area of directors' duties; investor protection and shareholder relief having appeared for the successful party in the leading BVI case on the use of directors' powers (*IAMC v SFL BVIHC COM 0034/2016*).

Jonathan is recognised as a "next generation partner" in the *Legal 500 2020 BVI Dispute Resolution* directory.

jonathan.addo@harneys.com

John McCarroll SC is of counsel in Harneys litigation, restructuring and insolvency group.

Prior to joining Harneys in 2018, John practised at the Chancery Bar in England and Wales (from 1988–2002) and the Bar of Ireland (2002–2018) working in commercial and chancery matters with a particular emphasis on company law, trusts, regulatory, insolvency, receivership and financial services.

John took silk in Ireland in 2013 and has 30 years' experience of appearing in the superior courts.

john.mccarroll@harneys.com

Christopher Pease is of counsel in Harneys litigation, restructuring and insolvency group. He advises on all aspects of commercial disputes and insolvency matters, with a particular specialism for disputes concerning fraud and bribery, asset recovery, applications for interim injunctive relief and applications for pre-action and third-party disclosure.

Prior to joining Harneys, Chris was a managing associate in the dispute resolution team at Linklaters in London. In his UK practice, Chris specialised in advising on complex fraud and contractual disputes as well as large-scale contentious regulatory matters, internal investigations and crisis management. As part of this practice, Chris advised on several successful settlement negotiations, including at mediation.

Chris is recognised as a "rising star" in *The Legal 500 2020 BVI Dispute Resolution* directory.

christopher.pease@harneys.com

Stuart Rau is a senior associate in Harneys litigation, insolvency and restructuring group. He advises on contentious cross-border matters covering multiple jurisdictions, including Europe, Asia, the US and the Caribbean.

Prior to joining Harneys in 2019, Stuart was of counsel at Allen & Overy in London and Hong Kong, where he focused on financial litigation and contentious regulatory matters.

stuart.rau@harneys.com

Harneys is a global offshore law firm with entrepreneurial thinking and a service built around professionalism, personal service and rapid response.

Harneys is expert in BVI, Cayman, Cyprus, Luxembourg, Bermuda and Anguilla law. The firm's lawyers are consistently recommended by leading independent legal directories such as *The Legal 500*, *Chambers and Partners*, *IFLR1000* and *Who's Who*.

Harneys advises an international client base which includes the world's top law firms, financial institutions, investment funds and private individuals.

Harneys network is one of the largest among offshore law firms, with locations in major financial centres in Europe, Asia, the Americas and the Caribbean, allowing it to provide services of the highest quality to clients in their own languages and time zones.

Harneys' associated corporate and private wealth services business, Harneys Fiduciary, is an independent provider of specialised corporate, trust and fiduciary services operating from key offshore and onshore locations around the world.

www.harneys.com

HARNEYS

Bulgaria

Angel Ganev
DGKV

Simeon Simeonov
DGKV

Lena Borislavova
DGKV

Over the past few years, cases of fraud, especially those facilitated by the modern technical means of communication (cyber frauds), have increased dramatically. In the most common scenario they have a cross-border nature, where the fraud is committed abroad, but the misappropriated assets (usually cash) are transferred to different jurisdictions worldwide, including Bulgaria.

This article will dissect the most common and widely used scheme of cyber fraud and its repercussion on a local level, as well as the mechanisms and statutory underpinnings for recovery within the legal framework of Bulgaria. It should be pointed out, however, that the main purpose of the article is not to analyse fraud from a criminal law perspective, but to present the following steps and legal solutions for the effective reimbursement of the victim and recovery of the misappropriated funds. Therefore, the emphasis will be placed on the *civil* remedies rather than the criminal analysis.

The article also highlights some of the key challenges and problems faced by local practitioners in the process of asset tracing and recovery, as well as the most effective ways to deal with them. In conclusion, some recent trends and developments will be also discussed.

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

A fraud has two main dimensions – a criminal and a civil one. The criminal dimension mainly deals with the detection and punishment of the offender, while the civil dimension is related to the recovery of misappropriated funds by their legitimate owner. Accordingly, there are two parallel and (relatively) independent layers of legislation in Bulgaria relating to fraud: asset tracing and recovery.

As regards the criminal aspect, the main pieces of legislation are the *Criminal Code* (CC) (promulgated, State Gazette No. 26/2.04.1968, effective 1.05.1968), the *Criminal Procedure Code* (CPC) (promulgated, State Gazette No. 86/28.10.2005, effective 29.04.2006) and the *Anti-Money Laundering Measures Act* (AMLMA) (Promulgated, State Gazette No. 27/27.03.2018, amended SG No. 94/13.11.2018, effective 1.10.2018); while the civil law aspect is covered by the *Law on Obligations and Contracts* (LOC) (Promulgated, State Gazette No. 275/22.11.1950, effective 1.01.1951), the *Civil Procedure Code* (CivPC) (Promulgated, State Gazette No. 59/20.07.2007, effective 1.03.2008) and the *Law on Credit Institutions* (LCI) (Promulgated, State Gazette No. 59/21.07.2006, effective 1.01.2007).

From a criminal law perspective, the CC provides for the legal definition of "fraud" and some specific types, while the CPC provides for the legal procedure followed by the competent authorities (investigation, prosecution and criminal courts) to pursue and charge the offenders.

The AMLMA, together with the CC, provides for the legal notion of *money laundering*, determined as a form of *subsequent* criminal activity (a predicate offence) and usually preceded by misappropriation of assets/funds. Whenever there is only a suspicion of money laundering and/or proceeds of criminal activity are involved, the AMLMA provides for the possibility of imposing conservatory measures by the civil court upon an explicit request made by the prosecution authorities. In the context of a fraud, followed by a potential money laundering case, the imposition of conservatory measures secures the satisfaction of a future claim of the state for confiscation of the property – subject of money laundering – if the latter is established by virtue of a final court decision.

The applicable civil legislation, however, is more complex. Thus, the LOC and CivPC provide for the principal set of civil substantive and procedural legal tools, while the LCI provides for some auxiliary legislation which is also relevant to the steps and ways of recovering misappropriated funds. Some other laws could also be of significance in the aftermath of a fraud, depending on the case (e.g. the *Code of Private International Law*, the *Bar Act*, the *Law on Commerce*, etc.).

In terms of civil substantive law, the LOC provides for specific legal claims and remedies, based on the *unjust enrichment* doctrine, which is a focal point in recovery schemes. According to this doctrine, any person who received something without cause, or for an unfulfilled or lapsed cause, must return it. In addition, when a person is enriched in any other way at the expense of another, the law imposes an obligation upon the recipient to make restitution. Under the relevant Bulgarian legislation, in the lack of legal relationship between the legitimate owner of the funds and the beneficiary (usually a part of the fraud scheme), the unjust enrichment doctrine serves as the only legal ground to claim the funds back from the recipient.

The LCI also contains some provisions, relevant to asset tracing and recovery schemes. More specifically, it establishes the notion of *bank secrecy*, which is especially important insofar as effective asset tracing is inevitably linked to the need of obtaining information from the local bank, especially during the first hours after commitment of a fraud. The LCI also provides for the possibility of lifting bank secrecy upon a court order in some specific cases.

As regards notable legal instruments, one of utmost importance is the *conservatory* (interim relief) measure, imposed by the civil courts under a procedure provided by the CivPC upon a request of the interested party, which aims at maintaining the *status quo* while the civil proceedings for recovery of the misappropriated funds are still pending. Another useful legal tool is the possibility for the claimant to request a *default judgment* (decision rendered *in absentia*), which is very common in fraud cases and subsequent civil actions, as fraudsters are normally not willing to reveal themselves to the public.

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

2.1 Cyber fraud: Modus Operandi

In its very essence, fraud is a false representation of a matter of fact by false or misleading conduct, for the purpose of acquiring material benefit for the fraudster or for another, resulting in a legal injury of the victim.

In recent years, however, a specific type of fraud has become widely popular, namely *cyber* fraud, or a fraud committed and facilitated by the modern ways of communication, such as the Internet. Cyber fraud contains all the elements of an "ordinary" fraud, adding some complexity with regards to the mechanism of execution, facilitated by specific technical means and devices.

A case of cyber fraud normally evolves from hacking the email or the entire computer system of a person, quite often a large international company with multiple business and income streams and headquarters spread worldwide, where the communication channels are mainly maintained electronically (i.e. through non-personal communication). After a time of observation of the hacked email/system, the attackers usually create a fraudulent

domain (a misspelt version of the original one). In fact, attackers use a palette of techniques, such as deployment of websites with real-like URLs, re-creation of attachments to genuine e-mails, using specialised software to make them visually identical, etc. From the fraudulent domain, the hackers start sending emails to the potential victims (the so-called *phishing*). In some cases, the victims are wealthy individuals, which are defrauded using a similar scheme. The ultimate victim, in the most common scenario, is a legal entity and a business partner with particular obligations to the one whose email/computer system is hacked. The deceiving messages could be sent by hackers either from the original email account or from another, posing as the original. In fact, the victim is deceived to effect a payment, usually due in the ordinary course of business between the parties so that no doubt will arise about the grounds for payment. The only difference set by the fraudsters is the *destination* of payment, which is normally in a remote jurisdiction, with Bulgaria being quite often among these places, along with Hong Kong, China and Singapore; in some cases, these are also the places of business of the victims. If questions are raised by the victim about the sudden change of destination and beneficiary, it is justified by various reliable excuses – technical reasons, current audit, etc. Accordingly, after a certain period of processing, the victim pays the requested amount to the newly designated bank account, by which the fraud is committed. The victim and its trusted party (who inadvertently helped the scheme) have nothing to do but to discover the malicious activity sooner or later and (eventually) report the fraud to the competent police and investigation authorities at the place of commitment. Undoubtedly, such schemes are often facilitated by an *insider*; however, for the purposes of this article we have not conducted specific research to that point.

In a specific group of cases, the victim is a financial director or controller (or holds a similar position) of a large multinational company, who is deceived to believe that a senior staff member asked him or her to effect a payment to a particular destination offshore (either with or without reasonable justification). In some rare instances, the false instructions could even be received over the phone.

The typical local beneficiary of the funds is a *shell* company, established by the fraudsters (usually shortly before the attack) for the sole purpose of absorbing the misappropriated funds and retransfer them later. The fictitious representative/s of the company usually stay hidden and in general refrains from public appearance for understandable reasons.

Cyber fraud is more complex than ordinary fraud as it involves a large number of parties (besides the fraudsters), institutions (large companies, banks) and last, but not least, multiple remote jurisdictions which, as a rule, handle the fraud and its consequences in a very different legal manner. Traditionally, in cases of cyber fraud, the misappropriated funds amount to millions.

2.2 Counter actions and recovery of funds

Whenever a fraud is detected and reported, there are some basic critical steps to be taken in order to secure eventual recovery of the misappropriated funds or at least to limit the damages: (a) establishing a contact with the local bank (the beneficiary's bank where the funds were transferred) in order to obtain the fullest possible information about the transaction; (b) imposing conservatory measures with a view to retaining the funds (if any) in the bank account; and (c) commencing civil action in order to recover the funds.

a) Establishing contact with the local bank

As it may be expected, once money has left the victim's account, it is transferred through multiple bank accounts in different jurisdictions, until final misappropriation by fraudsters. Logically, the local bank, which is the initial destination of the misappropriated funds, is the foremost source of information, especially with regard to the fundamental question as to whether the funds are still available in the bank at all. Other relevant information could be also obtained exclusively from the local bank, in particular details about the beneficiary (a future defendant in the civil action to be brought), the specific amount available, further

transfers, etc. If, unfortunately, at the time of the alert, the amount is no longer available in the designated account, the bank may at least provide the necessary information and documents to help chase the funds to other banks and jurisdictions. Lastly, the bank is the only proper source of information at this early stage about other potential freezing/injunction orders or other conservatory measures imposed by third parties (including measures imposed under the AMLMA upon the request of the prosecution authorities, see *Section 4* below) with regard to the same account and/or account holder, as they may significantly affect the recovery of the funds.

The most significant issue here is the reluctance of Bulgarian banks to provide information, mainly due to bank secrecy constraints and some other reasons. Bulgarian law does provide for an official legal definition of the term "bank secrecy". Pursuant to the LCI, the notion of bank secrecy embraces "*all facts and circumstances concerning balances and operations on accounts and deposits held by clients of the bank*". These include information on the person who opened and closed the account, the availability of funds, the transfers made within the country and abroad, dates and amounts, receiving accounts, the grounds for the transfers, as well as some other specific documents related to account balances and operations. On the other hand, the IBAN or any information related to bank loans or taxes are not covered by the definition of bank secrecy.

The protection granted to bank secrecy requires that this information is kept strictly confidential and is revealed to third parties, including law enforcement bodies, only in limited circumstances and in accordance with the procedural requirements described in the law. The main grounds on which bank secrecy can be revealed are provided for in LCI, but some sector-specific laws do contain additional grounds. With the 2015 amendments of the LCI, the law maker accommodated for a better legal framework in the context of civil fraud litigation cases, envisaging explicitly that bank secrecy can be revealed on the basis of a *court order*, when this information is of relevance for the case pending before the court. This allows for shorter timelines for tracing the assets, as the court order is not subject to an independent appeal procedure and is immediately enforceable.

The local bank is important, but not the only source of information. As Bulgarian law does not recognise the so called "search order", as known in some other jurisdictions, the only thorough and legitimate search of a debtor's property status could be made by the bailiff within already commenced foreclosure proceedings upon an explicit creditor's request. Yet, some limited public sources of information are available to the creditors, so that enforcement against potential additional assets of the debtor is secured. The checks which are normally conducted include verifications with the Commercial Register and the Register of Non-profit Legal Entities, as well as the Real Estate Register, maintained with the Registry Agency of the Republic of Bulgaria, the Central Special Pledges Register, held with the Ministry of Justice and the Central Depository (the latter maintains a register of book-entry shares, any transactions thereof and special pledges over the latter). However, our practice shows that the local recipient of a fraudulent payment barely has other property than the misappropriated funds.

b) Imposition of conservatory measures

If the misappropriated funds are still available with the local bank, the next important step is to secure the *status quo* until final settlement of the fraud case and the following civil claim. While not mandatory from a legal perspective, this step is strongly recommended as it guarantees that the funds will remain blocked until the legitimate owner, having successfully set out its case before a court of law, proceeds to enforcement against the misappropriated funds. Interim measures under Bulgarian law include freezing of bank accounts, attachments of movable assets, receivables and real estate property of the debtor, shares or company participations, suspension of forcible execution proceedings, transactions, etc.

An interim measure may be requested either *prior* to or *along* with the initiation of a civil lawsuit. Where it is obtained prior to initiation of claim proceedings, the court determines a deadline by

which the creditor should file its statement of claim against the debtor; this term may not be longer than one month. In the event of a failure by the creditor to initiate litigation by this deadline, the court will revoke the interim measure. The principal purpose of the interim relief injunction is that the debtor's assets remain frozen and cannot be transferred for the time the statement of claim is under review. Thus, by the imposition of interim relief at an earlier stage, the creditor gains a higher chance to receive payment of its receivables.

c) Initiation of civil action for recovery of the funds

Under Bulgarian law, ownership title when it comes to amounts of money (in cash or that available in a bank account) is evidenced by the fact of possession in the sense that the person who possesses the amounts shall be deemed their legitimate owner unless proven before a court of law that such person received the amounts without *just cause*. In the case of a fraud this means that, having received the funds under its account, the beneficiary/account holder shall be legally presumed the legitimate owner of the funds until proven otherwise before a court of law. The main implication of this (refutable) presumption is that, once the local account is officially *credited* with the funds, the bank may no longer unilaterally *withdraw* and return them to the sender (the defrauded party). Instead, the latter will have to resort to the civil court and to prove within ordinary civil proceedings that the funds were fraudulently wired from his or her account without legal cause whatsoever, and to seek a court decision ordering the account holder to pay the sum back. Therefore, the claim shall be based on the *unjust enrichment* doctrine and shall be brought before Bulgarian courts of law upon the statement that no legal relationship or other just cause underlies the fraudulent transfer and that the latter has been put into motion solely on the basis of a fraud committed against the victim.

In terms of timing, the decision of the first instance court is subject to appellate and cassation appeal, where the duration of the court proceedings may vary and often takes a long time which cannot be predicted, depending also on whether the parties appeal the court decisions on each instance. Based on our experience, the approximate timing for each instance may vary from approximately one to three years. Another important factor influencing the duration of judicial proceedings is whether the conditions for the claimant to request a default judgment are met. As already pointed out, it is very rare for the defendant to actively participate and defend in such cases. In the normal scenario, the defendant (the local beneficiary) does not react and no one reveals in the court. In this case, the CivPC provides for the possibility of rendering decision in absentia (a default judgment), if specific procedural prerequisites are met. The procedural conditions for the court to follow are: (i) the defendant has not submitted a statement of response within the statutory deadline; (ii) the defendant does not attend the first court hearing; (iii) the defendant has not declared explicitly that he wishes the case to be reviewed in his absence; and (iv) the claim is apparently founded. If the court favours the request for a default judgment, the latter enters into force *immediately* and significantly facilitates further recovery of the funds. Based on a positive judgment, entered into force, the creditor may obtain a writ of execution and launch foreclosure proceedings for recollection of the misappropriated funds.

3 Parallel proceedings: a combined civil and criminal approach

It is a common practice in Bulgaria that criminal and civil proceedings are initiated and pending simultaneously. As each of them has different purpose and development, they are relatively independent. Criminal proceedings are aimed at punishment of the offenders while the main goal of the civil proceedings is recovery of the funds. Although Bulgarian law allows the filing and review of a civil claim within criminal proceedings, due to a number of procedural specifics and time constraints, this option is either not applicable or not recommended.

In the most common scenario, the banks (both the local and the corresponding ones abroad) are the first to face signs of a fraud. Pursuant to the AMLMA, once a suspicious transaction (wire transfer) is detected, Bulgarian banks are obliged to report the case to the prosecution authorities and the director of the Financial Intelligence Directorate of the Bulgarian State Agency for National Security (SANS), which is normally followed by the initiation of a *criminal case* in the form of investigation proceedings, conducted by the competent authorities. Pursuant to the CPC, a criminal investigation (the first phase of a criminal case) might be commenced either upon a signal/warning letter, filed by any third person or *ex officio*, at the sole discretion of the prosecution authorities, if there is any available information concerning a crime committed. Importantly, in a standard case, criminal proceedings would be commenced for a money laundering crime rather than a fraud (please see *Section 4* below for the issues associated with this approach). Usually, at

the same time, the victim seeks legal assistance in the relevant jurisdiction where the money was transferred in an attempt to recover it.

Usually, in practice, a criminal proceeding will significantly hinder the civil one, mainly due to the fact that the prosecution in Bulgaria is slow, highly ineffective and suffers from a number of other shortcomings. On the other hand, as the criminal proceedings often precede the initiation of a civil case, the imposition of protective measures by prosecution authorities may be useful at the very beginning of a fraud case as it could potentially protect the money until further imposition of conservatory measures by the potential claimant. This is necessary as the interim measures, imposed by the prosecution authorities, could be lifted at any time without the knowledge and consent of the victim, upon the sole discretion of the prosecution authorities.

4 Key challenges

4.1 Time and information constraints

Needless to say, a key challenge in international fraud cases is the *time* factor. The electronic means of communication make wire transfers, transmission of messages, etc., happen literally in seconds. Very often, at the time the fraud is discovered, fraudsters have already managed to draw out the misappropriated funds. In such scenario, the options for an adequate response on a local level are very limited as the availability of the funds is an absolute precondition for any further recovery actions. Therefore, the connection with the local bank, the supply of sufficient information and the imposition of protective measures should happen literally within a day or two so that the victim has a bare chance of recovering the funds.

Another significant constraint is the lack of *information* at the time of receiving the first alert from the client. A lot of details are needed in order to initiate a viable action plan for recovery. As a first source of information, banks are very often reluctant to provide details as this could easily be viewed a breach of bank secrecy. In addition, legal practitioners are not equally positioned compared to the state investigation bodies which may, almost without limitation, receive information from all public and private institutions and other sources, including banks. Even more difficult, if not impossible, is the receiving of information from the prosecution authorities themselves, which, due to the specifics of criminal cases and for other reasons, firmly refuse to provide information, even to the victim. In such an adverse environment, the building of good relationships with local banks is necessary for legal practitioners in order to achieve successful assistance.

4.2 Parallel criminal proceedings and interim measures imposed under the AMLMA

Another key challenge in the process of recovering misappropriated funds is the pending criminal proceedings (usually in the form of preliminary investigation) at the time of starting recovery actions. Upon a signal for a suspicious bank transaction, the director of the State Agency for National Security (SANS) may issue a written order suspending it, in order to analyse the said operation or transaction and, eventually, confirm the suspicion. After carrying out the abovementioned analysis, the director shall inform the competent prosecution authorities, providing the necessary information. Following this information, the prosecutor may file to the competent

court a motion for imposition of conservatory measures, which usually (but not necessarily) take the form of attachment of immovable property or bank account/s. The intended purpose of such conservatory measures is to prevent transfers of money, acquired as a result of unlawful activity, so that the financial security of the Member States is secured. Pursuant to the binding case law of the Bulgarian courts, the prosecution authorities are entitled to request imposition and the court may favour such request even without the need of existence of a launched criminal investigation or a court procedure. The problem is that, due to the wide scope and legal possibilities of the AMLMA, the authorities tend to qualify any suspicious transaction (including obvious cases of fraud) as a money laundering case and to launch a criminal investigation on that ground. At the same time, the practice shows that such money laundering criminal cases are barely pursued by the authorities once they are initiated and the conservatory measures are imposed. Instead, in most of the cases, they are (unofficially) suspended immediately after initiation and no actual investigation activity is undertaken whatsoever. Since the pending criminal proceedings are the only ground for the validity of the attachment, until their official termination the attachment exists and hinders recollection of the funds by the victim (under the applicable law, attachments are executed in the order of their imposition). The only legal solution in such scenario is challenging the court ruling ordering the interim measure imposed by prosecution authorities; however, it may take considerable amount of time and struggle. The legal tool is a request for revocation of the conservatory measure, filed to the civil court which has imposed the attachment. It is only the civil court which deals with the matters related to the conservatory measures imposed under the AMLMA. Only the latter has the powers to reverse its own previous ruling for imposition and to lift the attachment. The entire process of filing a request before the court for lifting of the attachment and potential appeal in case the first instance court does not favour the request, may take roughly three to six months. If the appellate court upholds a potential negative court ruling, a request for lifting may be filed anew.

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

5.1 Relevant EU legal tools and mechanisms

EU legislation creates a number of legal tools which are also relevant to cross-border fraud cases. From a criminal law perspective, EU legislation guarantees that criminals can be pursued across borders and repatriated, thanks to the *European arrest warrant*. Judicial authorities cooperate through the European Union's Judicial Cooperation Unit (Eurojust) to ensure legal decisions made in one EU country are recognised and implemented in any other EU country. The EU also works to improve internal security and to have a coherent approach towards organised crimes. This includes taking action against organised criminals and helping national police forces work better together through the European Police Office (Europol).

In addition, the European Parliament and Council have adopted a regulation on the mutual recognition of freezing orders and confiscation orders (the new legal framework (Regulation (EU) 2018/1805) was published in the Official Journal of the EU of 28 November 2018 (O.J. L 303/1)). It establishes rules for the recognition and execution by a Member State of a freezing order issued by the judicial authority of another EU country in a *criminal* proceeding. This could either be a freezing order issued for the purpose of securing evidence in a criminal proceeding, or a subsequent confiscation order to permanently stop offenders from benefiting from their criminal conduct and prevent criminal property from being laundered or reinvested, potentially fuelling further criminality.

On a *civil* law level, a notable legal tool is *Regulation (EU) No 655/2014 of the European Parliament and of the Council of 15 May 2014 establishing a European Account Preservation Order procedure* to facilitate cross-border debt recovery in civil and commercial matters. The regulation establishes a unified procedure enabling a creditor to obtain a European account preservation order which prevents the subsequent enforcement of the creditor's claim from being jeopardised through the transfer or withdrawal of funds up to the amount specified in the order. However, in most cyber fraud cases, the fraud concerns persons located and funds originating from countries *outside* the EU. Thus, the regulation provided by the private international law and some international treaties shall also be applicable. For instance, pursuant to the Bulgarian Code of International Private Law (promulgated, State Gazette No. 42/17.05.2005), Bulgarian courts of law have jurisdiction to *secure* a claim over which they do not have international jurisdiction, if the subject matter of the conservatory measure is situated in Bulgaria and the anticipated judgment of the foreign court could be recognised and enforced in Bulgaria. The specific procedure for applying and obtaining a conservatory measure is again regulated by the CivPC (please see *Section 2.2(b)* above).

5.2 Unofficial channels of information and cooperation

Speaking about cross-jurisdictional mechanisms, the unofficial channels of information and cooperation could be in many cases very effective. As an example, the information exchanged through the corresponding international banks could be obtained long before the victim knew about the fraud and the competent authorities have commenced investigation. Another effective instrument, which is increasingly used in such cases, is the *private* criminal investigation, assisted by proper technical experts. The investigative and *digital* forensic support provided by them could often be a viable option for the victim in the process of obtaining timely information and asset tracing.

6 Technological advancements and their influence on fraud, asset tracing and recovery

The growing role of the Internet and new technologies in the context of cybercrimes and civil fraud is well recognised. On the one side, new technologies have drastically changed the ways of doing business; methods of communication between companies have shifted from traditional face-to-face interactions to that of email and other modern forms of communications, payments through electronic devices and different software applications are even more common than traditional payment methods, etc. These developments have increased the opportunities for fraud, which has inevitably increased the number of actual fraud cases and their diversity in relation to the mechanism of commitment.

On the other hand, however, new technologies are increasingly used to prevent and detect fraudulent transcations and behaviour. Improved system security, automated data analysis, data audit and risk assessment softwares, encryption, data mining, two-step verifications, and others serve for better and more efficient fraud detection and subsequent investigations. Nevertheless, the most crucial factor for effective recollection of the fraudulently acquired funds remains the fast intervention of the law enforcement bodies and legal practitioners involved.

7 Recent developments and other impacting factors

One of the most recent and important developments in the field of fraud, asset tracing and recovery is the EU proposal from the beginning of 2019 for a directive on combating fraud and counterfeiting of non-cash means of payment (including electronic wallets, mobile payments and virtual currencies). The directive is aimed at upgrading and modernising the existing rules in the fight against fraud in the EU Single Market. Some of the main provisions concern harmonised definitions of common online crime offences, such as hacking a victim's computer or phishing; as well as harmonised rules for penalties and clarifications of the scope of jurisdiction to ensure cross-border fraud is tackled more effectively.

Another recent development on a *local* level is the inclusion of computer-related crimes and frauds like phishing, other forms of social engineering and fake cryptocurrencies in the National Risk Assessment with respect to money laundering

activities, published by the SANS on 09.01.2020 (available in Bulgarian at https://www.dans.bg/bg/msip-091209-menu-bul/rezultatirisk-mitem-bg). SANS has allocated a medium level of risk (out of four levels of risks, indicated in the document) for these computer crimes on the territory of Bulgaria and has highlighted the existing difficulties for asset recovery. If a business, obliged to comply with the anti-money laundering legislation, establishes that they are exposed to this type and level of risk, they have to undertake appropriate measures and internal procedures to combat money laundering based on cybercrimes and civil fraud cases.

Angel Ganev heads the bankruptcy & insolvency and litigation & arbitration practice group at DGKV. His practice group includes more than 20 litigators specialising in complex commercial disputes and insolvency cases with a strong cross-border focus, as well as highly regarded asset recovery and anti-fraud subgroup. He is an experienced litigator with more than 18 years' practice in international arbitration, commercial litigation, and cross-border insolvency. Angel also acts on a regular basis as an arbitrator including in arbitration proceedings administrated by the ICC Court of Arbitration.

He also provides legal counsel to significant foreign investors on complex issues with regard to competence of courts, applicable law and recognition and enforcement of court judgments across borders.

Professional memberships: Sofia Bar; IBA; FraudNet; INSOL Europe; Member Chartered Institute of Arbitrators.

angel.ganev@dgkv.com

Simeon Simeonov is a senior associate and a proactive member of the litigation team, participating in the cornerstone disputes led by the law firm. He specialises in commercial litigation and insolvency. His professional experience encompasses civil and commercial litigation, including representation in a number of debt recovery court proceedings and public procurement procedures, consultations on mortgage secured bank loans, real estate law, etc.

simeon.simeonov@dgkv.com

Lena Borislavova is an associate at DGKV. A graduate of the Master's programme (LL.M.) in Law at Harvard Law School, USA. She specialises in mergers and acquisitions, commercial law, corporate governance and foreign investments. Lena assists major international companies in staying up to date with the latest local regulatory changes and applying the best practices for doing business in Bulgaria.

Lena is recognised in the 2018 European edition of *Forbes'* 30 Under 30 list of top young lawyers and policymakers.

lena.borislavova@dgkv.com

DKGV is one of the largest, oldest, and most prominent law firms in Bulgaria and provides a full range of legal services. Founded in 1994, the firm currently employs 54 lawyers, including 15 partners with extensive expertise. The law firm maintains offices in Sofia and Berlin. DGKV's major asset is its unique combination of profound legal knowledge, experience in complex international transactions and ability to handle large-scale transactions requiring simultaneous multidisciplinary approaches. The most respected international legal publications, such as *The Legal 500*, *Chambers & Partners*, *IFLR1000* and *Who's Who Legal,* recognise DGKV as a leading Bulgarian law firm.

www.dgkv.com

DJINGOV GOUGINSKI KYUTCHUKOV VELICHKOV
ATTORNEYS AND COUNSELLORS AT LAW

ICLG.com

COMPARE & RESEARCH THE LAW, WORLDWIDE.

Corporate Investigations 2020

IN PRINT AND ONLINE

This comprehensive guide provides practical, cross-border insights with expert analysis chapters written by leading legal practitioners, in addition to country-specific chapters in Q&A format, enabling readers to navigate, understand and cross-reference laws and regulations in key jurisdictions.

Contributing Editors:

Neil Gerrard
Dechert LLP

David Kelley
Dechert LLP

@ICLG_GLG

The International Comparative Legal Guides are published by: global legal group

Canada

Alexandra Luchenko
Blake, Cassels & Graydon

Sean Boyle
Blake, Cassels & Graydon

Iris Fischer
Blake, Cassels & Graydon

Simon Seida
Blake, Cassels & Graydon

Victims of fraud in Canada may avail themselves of a number of different remedies, whether they be criminal, administrative or civil.

Canada's constitution creates a division of powers between different levels of government, giving each the exclusive power to legislate within their respective heads of power. These powers are to be exercised within the confines of the *Canadian Charter of Rights and Freedoms* (Canadian Charter of Rights and Freedoms, Part 1 of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c. 11), which guarantees certain rights. All of Canada's provinces have systems based on the common law, with the exception of Quebec, a civil law jurisdiction. This chapter will focus on the most populous provinces of British Columbia, Alberta, Ontario and Quebec.

While each Canadian jurisdiction has its own statutory regimes, they share many similarities. Canada's *Criminal Code* (R.S.C. 1985, c. C-46) applies across the country. While the federal government enacts criminal law, the individual provinces and territories administer the system of enforcing it. This is contrasted from competition law, which the federal government both enacts and enforces itself. The provinces and territories are also responsible for implementing and enforcing their securities laws and have enacted statutes which provide for a variety of civil remedies and quasi-criminal sanctions for those found to be in violation of provincial securities laws, which may include fraud. In addition, any person defrauded by persons in regulated professions in Canada (such as doctors, lawyers, or realtors) may also complain to the regulatory body for the profession, possibly resulting in revocation of the professional's licence, the details of which are beyond the ambit of this chapter.

In the context of fraud and asset tracing, this framework has developed both a recognition of

the importance of protecting against fraud, but also ensuring that the rights of those accused of fraud are given due regard.

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

Criminal, administrative and civil proceedings are available in the context of fraud. Recovery schemes differ in each area.

Criminal proceedings

Statutory scheme

The language of the criminal offence of fraud found in the *Criminal Code* (section 380(1)) is broad. The provision allows investigating authorities the scope to cover a wide array of potentially fraudulent conduct. The offence requires two essential elements: dishonesty on the part of the fraudster and a corresponding deprivation to the fraud target (*R. v. Olan*, [1978] S.C.J. No. 57, [1978] S.C.R. 1175 at 1182). In addition to the main fraud offence, there are several ancillary offences aimed at specific situations and parties who assist fraudsters in advancing their activities (See: *Criminal Code*, R.S.C. 1985, c. C-46, ss. 380-396).

In Canada, the Royal Canadian Mounted Police ("RCMP") are responsible for investigating criminal fraud in many jurisdictions (*Royal Canadian Mounted Police Act*, R.S.C. 1985, c. R-10, ss. 18, 20). However, certain provinces (including Ontario and Quebec) and most large municipalities have their own police forces responsible for investigating criminal misconduct within their jurisdiction. Provincial attorney general offices (referred to as the "Crown") are responsible for prosecuting offences. Police forces have the power to seize property and assets. These powers require the police to have reasonable grounds that the asset was used in or obtained as a result of a breach of criminal or other statutory law (*Criminal Code*, R.S.C. 1985, c. C-46, s. 489).

There are also several quasi-criminal regulators which have the power to investigate certain types of fraud. For example, provincial securities regulators are empowered to investigate and prosecute fraudulent trading in securities. Each of these provincial regulators generally has the power under their enabling statutes to seize or enter property for the purpose of carrying out their investigations. The federal Competition Bureau similarly has the power to investigate and prosecute certain types of consumer fraud such as deceptive marketing or anti-competitive market conspiracies and has the same powers to seize and enter property (*Competition Act*, R.S.C. 1985, c. C-34, ss. 10, 11, 14.1, 15, 45, 52).

Recovery

Following the conviction of a fraudster, the Crown may seek criminal forfeiture of any assets of the fraudster used in or acquired as a result of the fraud. Such forfeiture may either be mandatory or discretionary (*Criminal Code*, R.S.C. 1985, c. C-46, s. 490.1). The Crown may also seek criminal forfeiture of any assets of a fraudster acquired as a result of the fraud where the accused is not available for trial (*Criminal Code*, R.S.C. 1985, c. C-46, s. 490.2).

Following a criminal conviction, a court may also order a restitution order (*Criminal Code*, R.S.C. 1985, c. C-46, s. 738). These orders require an offender to pay to the target of their crime a sum of money to compensate for the financial loss they suffered. Restitution orders are discretionary. They are ordered based on a multitude of factors which depend on the circumstances of each individual case. Restitution orders are not meant to be a substitute for private law remedies such as damages (*R. v. Trac*, 2013 ONCA 246 at paras. 32-36).

Eight of the 10 provinces and the territory of Nunavut have also enacted legislation creating a statutory remedy for provincial authorities to recover the proceeds of crime to supplement the forfeiture powers available under the *Criminal Code* (See: *Victims Restitution and Compensation Payment Act*, S.A. 2001, c. V-3.5; *Civil Forfeiture Act*, S.B.C. 2005, c. 29; *The Criminal Property Forfeiture Act*, S.M. 2004, c. 1; *Civil Forfeiture Act*, S.N.B. 2010, c. C-4.5; *Civil Forfeiture Act*, S.N.S. 2007, c. 27; *Unlawful Property Forfeiture Act*, S.Nu. 2017, c. 14; *Civil Remedies Act, 2001*, S.O. 2001, c. 28; *Act respecting the forfeiture, administration and appropriation of proceeds and instruments of unlawful activity*, CQLR, c. C-52.2; *The Seizure of Criminal Property Act, 2009*, S.S. 2009, c. S-46.002). This is commonly known as civil forfeiture.

While the formal procedures and statutory prerequisites for provincial forfeiture proceedings vary across the jurisdictions, the general concept is consistent. Civil forfeiture laws allow the seizure and transfer of property when the property is suspected of being used to commit an illegal act or is suspected of having been acquired by committing an illegal act. Unlike criminal proceedings, civil forfeiture proceedings are *in rem*, meaning they are taken against the property itself and not any specific individual. The Crown or other prosecuting authority is not required to prove any particular offence against any particular offender, only that some wrongdoing occurred (*Ontario (Attorney General) v. Chatterjee*, 2009 SCC 19 at paras. 19-23. It is important to note that this decision was dealing with Ontario legislation, however, the principles discussed have application throughout Canada. See also: *British Columbia (Director, Civil*

Forfeiture) v. Vo, 2013 BCCA 279 at paras. 22-26; *Québec (Procureur général) c. 9148-5847 Québec inc.*, 2012 QCCA 1362 at paras. 56-59; *Saskatchewan (Director under the Seizure of Criminal Property Act, 2009) v. Mihalyko*, 2012 SKCA 44 at paras. 17-18; *Alberta (Minister of Justice & Attorney General) v. Pazder*, 2010 ABCA 183 at paras. 9-10).

Administrative proceedings

Securities fraud

Provincial legislation regulating securities contain provisions regarding fraud for the purposes of investor protection overseen by the securities commission of a given jurisdiction. The investigatory powers of such commissions allow regulators to compel production of evidence and freeze assets prior to a hearing. Breaches of securities' legislation can lead to civil or criminal responsibility for the offender.

Certain offences prosecuted by securities regulators are "quasi-criminal" proceedings and can carry a jail term of up to five years, a fine up to $5 million CAD, or both for each conviction, depending on the jurisdiction. Generally, such proceedings are reserved for egregious violations.

Administrative penalties are a common remedy used by securities regulators in contrast to quasi-criminal convictions. Securities regulators may impose an administrative penalty of up to $1 million CAD for each breach of securities legislation, depending on the jurisdiction. Given the lower standard of proof in administrative proceedings, administrative penalties are increasingly becoming the preferred remedy for securities regulators throughout Canada.

Competition fraud

The federal Competition Bureau is the administrative body responsible for enforcing Canada's competition laws. Breaches of competition laws, similarly to securities laws, can lead to civil or criminal responsibility for the offender. The *Competition Act* contemplates a broad range of conduct that comes under the jurisdiction of the Competition Bureau which may be subject to sanctions, including fraudulent and deceptive practices (See: *Competition Act*, R.S.C. 1985, c. C-34, ss. 52-52.01, 52.1, 53-55.1, 74.01-74.06). Similarly to the provincial securities regulators, the Competition Bureau has broad investigatory powers to compel testimony, production of documents and in some cases freeze assets (*Competition Act*, R.S.C. 1985, c. C-34, ss. 10-12, 14.1-16, 20, 74.111).

The Competition Bureau also generally can prosecute using either administrative proceedings or criminal proceedings. The maximum criminal penalties vary with the individual offence but can be up to 14 years in jail and significant monetary fines for the most severe offences (*Competition Act*, R.S.C. 1985, c. C-34, ss. 52-52.01, 52.1, 53-55.1). The maximum administrative penalties for corporate offenders are $10 million CAD for a first breach and $15 million CAD for every subsequent breach, and for individuals are $750,000 CAD and $1 million CAD, respectively. These administrative penalties are in addition to any prohibitions on conduct the Competition Bureau may require (*Competition Act*, R.S.C. 1985, c. C-34, s. 74.1).

Civil proceedings

Private parties who suffer fraud can seek compensation by commencing a civil lawsuit for a number of different causes of action, including general fraud, fraudulent misrepresentation, breach of fiduciary duty (if the fraud took place in the context of a specific relationship), unjust enrichment, knowing assistance or conversion. In Quebec, civil fraud is codified by the *Civil Code of Quebec* (for example: *Civil Code of Quebec*, S.Q. 1991, c. 64, as. 316-317). Throughout Canada, claimants commencing a legal proceeding must specifically plead a cause of action in fraud and must typically provide "full particulars" of the fraud (See: *Alberta Rules of Court*, Alta. Reg. 124/2010, s. 13.7; *Supreme Court Civil Rules*, B.C. Reg. 168/2009, s. 3-7(18); *Court of Queen's Bench Rules*, Man. Reg. 553/88, s. 25.06(11); *Rules of Court of New Brunswick*, N.B. Reg. 82073, s. 27.06(9); *Rules of the Supreme Court, 1986*, S.N. 1986, c. 42, Sched. D, s. 14.11(1)(a); *Rules of the Supreme Court of the Northwest Territories*, N.W.T. Reg. R-010-96, s. 117; *Nova Scotia Civil Procedure Rules*; N.S. Civ. Pro. Rules 2009, s. 38.03(3); *Rules of Civil Procedure*, R.R.O. 1990, Reg. 194, s. 25.06(8); *Rules of Civil Procedure*, P.E.I. Rules, S. 25.06(8); *The Queen's Bench Rules*, Sask. Q.B. Rules 2013, Pt. 13, S. 13-9(1)).

Interlocutory orders

There are certain applications that may be made either before starting a proceeding or in advance of full judgment being rendered that may protect or assist a claimant in prosecuting an action by obtaining evidence or preserving assets prior to dissipation. Whether such avenues are appropriate from a practical perspective, or even available at law, will depend on several factors as set out below.

Norwich order

It is often challenging to identify the perpetrator of a fraud. In such cases, a claimant can seek a *Norwich* order, even if legal proceedings have not been commenced. A *Norwich* order compels a third party to produce information that can assist identifying a wrongdoer (*Tetefsky v. General Motors Corp.*, 2010 ONSC 1675 at paras. 33-35). *Norwich* orders can be very helpful in determining if a fraud has occurred, identifying the fraudster or tracing the assets stolen.

The *Norwich* order is an extraordinary remedy and is not granted lightly (*B. (A.) v. D. (C.)*, 2008 ABCA 51 at paras. 7, 15). The factors considered by courts in determining if a *Norwich* order is appropriate are:

1. whether the applicant has a valid, *bona fide* or reasonable claim;
2. whether the applicant has established a relationship to the third party that shows the third party is involved in the acts complained of;
3. whether the third party is the only source available for the information sought;
4. whether the third party can be indemnified for costs because of the exposure of the information; and
5. whether the interests of justice favour granting the relief. (*Tetefsky v. General Motors Corp.*, 2010 ONSC 1675 at para. 36.)

A *Norwich* order can be obtained even if the target did not intentionally play a part in the fraud (*Tetefsky v. General Motors Corp.*, 2010 ONSC 1675 at paras. 33-35. See also: *B. (A.) v. D. (C.)*, 2008 ABCA 51 at para. 12). Banks, internet service providers and telecommunications companies are typically the respondents to applications for *Norwich* orders.

Anton Piller orders

Claimants may also be able to collect evidence against a defendant accused of fraud by obtaining an *Anton Piller* order. *Anton Piller* orders allow a claimant in a lawsuit to search the defendant's property in order to obtain relevant evidence. There are four requirements to obtain an *Anton Piller* order:

1. the plaintiff must demonstrate a strong *prima facie* case of fraud;
2. the potential or actual damage to the plaintiff by the defendant's alleged conduct must be very serious;
3. the plaintiff must show evidence that the defendant has the incriminating evidence in their possession; and
4. there must be a real possibility that the defendant may destroy the evidence before the discovery process advances. (*Celanese Canada Inc. v. Murray Demolition Corp.*, 2006 SCC 36 at paras. 1, 35-38.)

Generally, given the intrusive nature of the remedy, courts will require that an independent lawyer conduct the search (*Celanese Canada Inc. v. Murray Demolition Corp.*, 2006 SCC 36 at para. 40).

Mareva injunctions

If the person suspected of perpetrating a fraud has known assets, a *Mareva* injunction may be considered. A *Mareva* injunction freezes eligible assets. *Mareva* injunctions are generally sought *ex parte*, meaning the other party is not given notice of the claimant's attempt to obtain the order to prevent dissipation (*Aetna Financial Services Ltd. v. Feigelman*, [1985] 1 S.C.R. 2, 1985 CarswellMan 19 at para. 19 (S.C.C.). See also: *SFC Litigation Trust (Trustee of) v. Chan*, 2017 ONSC 1815 at para. 61). To obtain a *Mareva* injunction, the plaintiff must:

1. establish a *prima facie* case of fraud (*SFC Litigation Trust (Trustee of) v. Chan*, 2017 ONSC 1815 at paras. 17, 60);
2. establish the defendant has some assets within the court's jurisdiction (*Aetna Financial Services Ltd. v. Feigelman*, [1985] 1 S.C.R. 2, 1985 CarswellMan 19 at para. 19 (S.C.C.). See also: *SFC Litigation Trust (Trustee of) v. Chan*, 2017 ONSC 1815 at paras. 17, 60);
3. establish that there is a risk of assets being

dissipated from the jurisdiction before judgment (*Aetna Financial Services Ltd. v. Feigelman*, [1985] 1 S.C.R. 2, 1985 CarswellMan 19 at paras. 29-30 (S.C.C.). See also: *SFC Litigation Trust (Trustee of) v. Chan*, 2017 ONSC 1815 at para. 17, 60);

4. establish irreparable harm to the plaintiff if the injunction is not granted (*HZC Capital Inc. v. Lee*, 2019 ONSC 4622 at para. 45);
5. establish that the balance of convenience requires the granting of the injunction (*HZC Capital Inc. v. Lee*, 2019 ONSC 4622 at para. 45); and
6. give an undertaking to account for any damages that may result from the improper granting of the order (*SFC Litigation Trust (Trustee of) v. Chan*, 2017 ONSC 1815 at paras. 9, 17, 60).

While the test is arduous, Courts have indicated that the risk of dissipation of assets may be inferred from the circumstances in appropriate cases (*2092280 Ontario Inc. v. Voralto Group Inc.*, 2018 ONSC 2305 at para. 23). In some cases, *Mareva* injunctions may be issued for worldwide assets (*SFC Litigation Trust (Trustee of) v. Chan*, 2017 ONSC 1815 at para. 38). A *Mareva* injunction does not attach to the assets themselves, but to the defendant (*SFC Litigation Trust (Trustee of) v. Chan*, 2017 ONSC 1815 at paras. 27-30).

A *Mareva* injunction is another extraordinary remedy that is not granted lightly given the profound effect that it may have on a defendant and their ability to manage their assets (*SFC Litigation Trust (Trustee of) v. Chan*, 2017 ONSC 1815 at para. 57).

Certificate of pending litigation

if the proceeds of fraud can be traced to real property somewhere in Canada, then a claimant may seek a certificate of pending litigation after commencing proceedings (see for example: *Courts of Justice Act*, R.S.O. 1990, c. C.43, s. 103).

A certificate of pending litigation allows a plaintiff to register a charge on title against real property in the name of the person that allegedly perpetrated the fraud if the allegation discloses a claim for an interest in land. This charge serves as a notice to anyone seeking to purchase the land from the fraudster that the claimant has made a claim for the land which may result in the fraudster no longer having title to the land. Practically-speaking, few purchasers will acquire land subject to such a charge (*G.P.I. Greenfield Pioneer Inc. v. Moore*, [2002] O.J. No. 282, 2002 CarswellOnt 219 at paras. 15-16 (ON CA)). In Quebec, there is a similar concept called an advance registration (*Civil Code of Quebec*, S.Q. 1991, c. 64, as. 2966-2968).

Remedies

Damages

Claimants will first seek monetary damages attributable to the fraud. Aggravated damages are also often sought because of the conduct of a fraudster on their mental wellbeing. Aggravated damages are a type of compensatory damages aimed at compensating for the intangible injuries suffered by a claimant, such as mental distress or loss of enjoyment, caused by the conduct of the defendant. These damages are awarded in cases where the fraudster's conduct was particularly high-handed or oppressive and increased the claimant's humiliation or anxiety (*Hill v. Church of Scientology of Toronto*, [1995] 2 S.C.R. 1130, 1995 CarswellOnt 396 at paras. 191-193 (S.C.C.). See also: *Fidler v. Sun Life Assurance Co. of Canada*, 2006 SCC 30 at paras. 51-52).

In certain circumstances, courts may also award a claimant punitive damages if the conduct of the fraudster is malicious, oppressive and high-handed and offends the court's sense of decency. Punitive damages are not compensatory in nature as they are intended to punish, deter and denounce the conduct of the fraudster (*Whiten v Pilot Insurance Co.*, 2002 SCC 18 at paras. 36, 68-69).

Constructive trust

Constructive trusts have been imposed to prevent unjust enrichment of defendants and for otherwise wrongful acts (*Moore v. Sweet*, 2018 SCC 52 at para. 26). Essentially, they create a proprietary right to assets held by a fraudster and the fraudster is deemed the trustee of the assets for the benefit of the claimant. This can give rise to fiduciary obligations akin to any other trustee (*Soulos v. Korkontzilas*, [1997] 2 S.C.R. 217, 1997 CarswellOnt 1489 at paras. 17-20 (S.C.C.)).

Accounting

An account of profit seeks to disgorge the fraudster of their ill-gotten gains which rightfully belong to the claimant. This remedy is measured according to the fraudster's gain, it is not measured by the fraudster's gain in relation to the claimant (*Lac Minerals Ltd. v. International Corona Resources Ltd.*, [1989] 2 S.C.R. 574, 1989 CarswellOnt 126 at para. 67 (S.C.C.)). This remedy is generally applied in cases involving breach of fiduciary duty, such as the duties of a trustee. There must be a causal relationship between the breach and the ill-gotten profits (*Genesis Fertility Centre Inc. v. Yuzpe*, 2019 BCSC 233 at paras. 315-316 citing *Strother v/ 3464920 Canada Inc.*, 2007 SCC 24 at para. 79).

Equitable charge or mortgage

When a fraudster has implicated real property in a fraud in such a way as to deprive a mortgagee

or creditor of their interests, a court may order an equitable charge or mortgage over the title to preserve the interest which would otherwise no longer exist at law. Such charges arise where there is a common intention of the mortgagor and mortgagee to secure property for a past or future debt and where the intention is unenforceable at common law (*O'Brien v. Royal Bank,* [2008] O.J. No. 653, 2008 CarswellOnt 910 at paras. 24-25 (ON SC). See also: *League Assets Corp., Re*, 2015 BCSC 42 at paras. 64-67).

Appointment of receiver-manager

In cases of corporate fraud, it may be appropriate to seek a receiver-manager over the corporate assets. The appointment of a receiver-manager generally ousts the power of a board of directors to manage the assets of a corporation and vests in the receiver-manager the power to collect income and manage the affairs of the corporation (See for example: *Canada Business Corporations Act*, R.S.C. 1985, c. C-44, ss. 94-96). Receiver-managers may be sought under a variety of statutory enactments throughout Canada, particularly under securities laws, and even under equitable doctrines.

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

Civil cases are the focus of this section. Criminal and administrative proceedings are driven not by private parties but the Crown or representatives of the administrative body in question.

Following the discovery of a fraud, victims will often be forced into a sort of triage as they attempt to understand the nature and scope of the fraud while also making attempts to contain it. In the investigatory stage, decisions will quickly need to be made whether the perpetrator can be identified, whether action should be taken and whether to involve regulatory or criminal law enforcement. These decisions must be taken quickly to maximise the potential of recovery (a significant concern in litigation involving fraud). While quick action is preferable in such circumstances, it is important to note that fraud claimants generally have up to two years from the date they discover the fraud to bring proceedings. Discovering the fraud means that they are aware they have been wronged and that legal proceedings are an adequate remedy for the wrong.

The civil litigation process in Canada is adversarial in nature and thus not always well-suited to providing tangible remedies to victims if a perpetrator is effective at hiding their assets or absent an order preserving assets (such as a *Mareva* injunction). The documentary and oral discovery process may provide further evidence of the fraud assuming the alleged perpetrator abides by their obligations, is forthright and took action that can be discerned by studying records.

Following a successful civil suit, the claimant will generally be awarded damages for their loss or restitution from the fraudster. The claimant must then attempt to collect the award, which may be particularly challenging. Successful claimants have certain enforcement mechanisms available to them to enforce a judgment. If the claimant obtained the financial information of the fraudster during the litigation, then they would be aware of these assets. This can allow the claimant to execute against those assets, seek garnishment of those assets, register charges against those assets or even appoint receivers over those assets in some rare instances. If still unaware of the assets of the fraudster following judgment, claimants can seek examination of the fraudster under oath to learn of their finances.

Parallel proceedings: A combined civil and criminal approach

Under section 11 of the *Criminal Code*, no civil remedy is suspended or affected by the fact that an act or omission is a criminal offence. This means that no person is precluded from bringing a civil claim against a fraudster simply because the fraudster is also facing criminal charges. It is common for parallel proceedings to occur for fraudulent activities. The same is generally true for concurrent civil and administrative proceedings.

Increasingly, the trend is for concurrent civil and administrative hearings to arise out of the same fraudulent conduct, particularly in the securities and competition law contexts. The greatest advantage in a combined approach for a private claimant is the potential reduction in investigation and litigation costs.

If criminal or administrative proceedings are commenced against an alleged fraudster, depending on the circumstances, a claimant may allow the Crown or other prosecuting authority to conclude their proceedings prior to taking steps in their civil proceeding. Claimants can seek disclosure of evidence collected by the police or administrative prosecution through a *Wagg* order, although there are generally significant privilege and confidentiality concerns that accompany such disclosures (*P. (D.) v. Wagg*, 71 O.R. (3d) 229, 2004 CarswellOnt 1983 at paras. 48-55 (ON CA). For adoption in other provinces see: *Feuerhelm v. Alberta (Justice and Attorney General)*, 2017 ABQB 709 at para. 112; *Dudley Estate v. British Columbia*, 2016 BCCA 328 at para. 108; *LeBlanc c. Haché*, 2014 NBBR 99 at para. 46; *T. (S.) v. T. (J.)*, 2015 SKQB 249 at paras. 16-17). Further, any findings of culpability of the fraudster in these administrative or criminal proceedings can properly be adduced as evidence of wrongdoing in any subsequent civil claim. However, depending on the time sensitivity of the action, waiting may ultimately harm the claimant, for example due to asset dissipation.

Key challenges

Fraud is by definition designed to be clandestine, leading to a significant deficit of information on the part of the claimant. Proving a fraud is rarely the challenge. Without being able to identify a perpetrator or actually recoup assets, a victory in Court will be hollow. In fact, due to the cost of legal proceedings, the claimant may simply have thrown good money after bad.

The use of innocent intermediaries and dummy accounts are just some examples of how fraudsters distance themselves from their actions. A

potential fraudster may not legally or beneficially own any interest in the asset a claimant is seeking to recover.

Additionally, the cost of legal proceedings and enforcing subsequent judgments has always been a challenge in this area. Seeking many of the aforementioned civil remedies is onerous and the cost of the legal work to adequately prepare for such applications can be substantial. This is coupled with the slow pace of civil litigation in Canada. It is not uncommon for a civil fraud case to drag on for two or more years. The cost of retaining competent counsel during this period can add up. If the result is a hollow victory, the cost of getting to judgment may end up being greater than the recovery itself, particularly if the claimant must then exert resources attempting to recover their award.

Securities regulators throughout Canada particularly struggle in recovering penalties for securities offences, fraud-related or otherwise. For example, the collection rate for penalties imposed for financial crimes by the British Columbia Securities Commission was reportedly less than 2% during the 2016/2017 fiscal year (British Columbia Securities Commission, *2016/2017 Annual Service Plan Report*, (Vancouver: British Columbia Securities Commission, 2017) at 48, online: British Columbia Securities Commission).

A separate type of challenge exists in the context of civil forfeiture. Such a remedy can create many difficulties for unwitting individuals who are implicated by another's fraud. The low standards of proof allow governments to seek forfeiture of assets with relative ease. British Columbia's statute does not even require a hearing for property worth less than $75,000 (called an "administrative forfeiture") and the appeal period is fairly short (*Civil Forfeiture Act*, S.B.C. 2009, c. 29, Part

3.1). Often by the time the private citizen knows their property has been seized, the appeal period has passed. Sometimes the value of the property seized is negligible, making the legal costs of disputing the forfeiture impractical. While other provinces do not have British Columbia's extreme form of forfeiture, they nonetheless have statutes that are skewed towards simplifying forfeiture for government bodies, which has been the subject of some critique by certain groups.

Cross-jurisdictional mechanisms: Issues and solutions in recent times

Collection of evidence for foreign proceedings

In the context of civil proceedings, those seeking assistance from the Canadian courts to compel evidence in Canada must obtain and enforce letters rogatory, also known as letters of request or evidence under commission. Letters rogatory are essentially requests from a foreign court to the local court to assist the foreign court in obtaining evidence within the local court's jurisdiction. The provincial and federal evidence legislations throughout Canada specifically contemplate letters rogatory and the basis for granting these requests. While the specific factors and statutory preconditions relevant to enforcing letters rogatory vary slightly from province to province, throughout Canada the overriding concern for local courts are two-fold:

1. what is the impact of enforcing the order on Canadian sovereignty; and
2. does justice require the taking of evidence be ordered?

Enforcing foreign judgments

A judgment obtained by a claimant in another jurisdiction can be enforced in Canada as if it were a judgment of a local court, if it is registered as a judgment and meets certain requirements (which vary across the jurisdictions). Judgments from reciprocating jurisdictions need only be registered to be enforced. As such, a claimant that has already sued abroad and obtained a judgment may come to Canada in order to collect payment for damages and, in some cases, enforce non-monetary judgments.

Criminal and regulatory matters

With respect to criminal matters, the *Mutual Legal Assistance in Criminal Matters Act* (R.S.C. 1985, c. 30 (4th Supp.)) (*MLACMA*) addresses cross-jurisdictional mechanisms. *MLACMA* outlines the procedure and preconditions for local governments to assist foreign states in gathering evidence or enforcing arrest, search, seizure or forfeiture orders for criminal matters (See for example: *MLACMA*, R.S.C. 1985, c. 30 (4th Supp.), ss. 9.3-23). If the statutory preconditions are not met, Canada may refuse to enforce orders generally or specifically for various reasons including public policy.

In the regulatory context, British Columbia, Alberta, Ontario and Quebec are all party to the International Organization of Securities Commissions' Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information. These four provinces, along with many of the other provinces, are also party to similar agreements with the United States' Securities and Exchange Commission. Under these agreements, the securities commissions provide one another with mutual assistance by providing access to commission files, taking evidence and obtaining documents necessary for investigations. The agreements do not create any specific framework but operate within the legal frameworks already in place in all the jurisdictions. In this light, any evidence collected by most Canadian securities commission will be made available for foreign securities regulators based on the terms of the specific agreements in effect.

The federal Competition Bureau similarly has mutual legal assistance provisions in its enabling statute. These provisions allow for orders for gathering evidence, searches and seizure of assets (*Competition Act*, R.S.C. 1985, c. C-34, ss. 30-30.3). The federal Competition Bureau also, like securities regulators, has agreements with foreign counterparts to facilitate cooperation and coordination in cross-border competition enforcement matters. These agreements allow for the sharing of information and the coordination of joint enforcement mechanisms and procedures in order to achieve the enforcement goals of all signatories.

Technological advancements and their influence on fraud, asset tracing and recovery

Advancement in technology has helped in combatting fraud, but has also facilitated increasingly sophisticated schemes. Increased phishing and cyber-attacks are leading to a greater emphasis on "tech hygiene" so that people and companies are kept safe. The use of virtual currencies for money laundering and fraudulent transactions is only a recent example of how technological developments, while exciting, allow fraudsters new and creative ways to defraud the public.

It remains to be seen how Canadian markets and commerce will respond to a growing cryptocurrency market and increased regulation in this area. Securities regulators are only now grappling with the issues of regulating this industry and have recently introduced rules on how cryptocurrencies are to be publicly traded.

Recent developments and other impacting factors

New legislation

The Canadian government introduced amendments to its *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (S.C. 2000, c. 17) which should curtail certain fraudulent transactions (*an Act to implement certain provisions of the budget tabled in Parliament on March 19, 2019 and other measures*, S.C, 2019, c. 29, ss. 98-126). Canada had been known for its lax money laundering laws and the amendments were an attempt to bring Canada up to par with its contemporaries. The changes addressed issues such as the use of prepaid credit cards, virtual currencies, electronic fund transfers, reporting of suspicious transactions, and 24-hour transaction rules. All these areas of regulation have historically been used as a means for money laundering and fraudulent activity. The changes will now provide stricter control measures on specific financial products, as well as higher reporting standards to reduce laundering of proceeds from unlawful activities.

The *Criminal Code* was also recently amended to allow for the use of remediation agreements, also known as deferred prosecution agreements in the United States (See: *Criminal Code*, R.S.C. 1985, c. C-46, ss. 715.3-715.43). These will allow accused corporations an opportunity to negotiate with prosecutors if it is in the public interest. The hope is that corporations will voluntarily reveal wrongdoing such as fraud so as the minimise its impact and to mitigate any further wrongdoing. These agreements allow corporations to reduce criminal liability so long as they uphold the terms of the agreement.

The British Columbia government recently passed amendments to its securities laws in order to give the British Columbia Securities Commission stronger enforcement and collection tools. The new laws no longer require the British Columbia Securities Commission to have hearings before imposing administrative penalties, allowing them to now do so *ex parte*. The changes also allow for seizure of property owned by immediate family of wrongdoers, even if the wrongdoer has no ownership interest. These changes, which are unprecedented in Canada, are an attempt to bolster the ability of the British Columbia Securities Commission to enforce and collect penalties and to streamline the process while reducing alleged wrongdoers' abilities to frustrate proceedings and penalties. It remains to be seen if other provinces will follow suit, but Ontario has indicated it is considering rehauling its *Securities Act* (Ontario, Legislative Assembly of Ontario, *Hansard*, 42nd Parliament, 1st session, Volume A (25 November 2019) at 6272).

Jurisprudence

In a recent Supreme Court of Canada case, *Saloman v. Matte-Thompson* (2019 SCC 14), the Court ordered a lawyer and his law firm to fully compensate his clients for losses suffered as a result of a fraud perpetrated by a financial advisor referral by the lawyer (*Salomon v. Matte-Thompson*, 2019 SCC 14 at paras. 1, 5-6). The decision confirms that fraud committed by a third party will not always shield such third party from liability (*Salomon v. Matte-Thompson*, 2019 SCC 14 at paras. 91-92. See also: *Cole Parliament et al. v. D.W. Conley and V. Park*, 2019 ONSC 3996 at paras. 19-28).

The Supreme Court of Canada also recently provided light on the doctrine of "knowing assistance" in *Christine DeJong Medicine Professional Corp. v. DBDC Spadina Ltd.* (2019 SCC 30). Knowing assistance is intentionally and knowingly (or being reckless or wilfully blind thereof) assisting a fiduciary in fraudulent or dishonest conduct in breach of the fiduciary's duties (*DBDC Spadina Ltd. v. Walton*., 2018 ONCA 60 at paras. 211, 216; *Caja Paraguaya De Jubiliciones Y Pensiones Del Personal De Itaipu Binacional v. Garcia*, 2018 ONSC 5379 at para. 441). It is often used to catch those who were not involved in the fraud but had actual knowledge of it. The Supreme Court of Canada affirmed that participation and assistance require more than passive involvement in the fraudulent conduct to attract liability. Being a conduit for a fraudster is not sufficient to establish liability (*DBDC Spadina Ltd. v. Walton*., 2018 ONCA 60 at paras. 230-231, 236-237).

Alexandra Luchenko has a particular interest in fraud and asset recovery cases, with experience investigating fraud claims through to enforcement and collections. Alexandra has been involved in numerous investigations involving cross-border aspects as well as cybersecurity-related matters. She has considerable experience working with financial institutions, as well as clients in the mining, resource, technology and health sciences industries. She is a Certified Fraud Examiner and regularly collaborates with other experts to deliver the best possible results for clients requiring crisis management advice. Alexandra has complementary experience in securities litigation, complex corporate/commercial litigation regulatory compliance and advising on compliance with anti-corruption legislation in Canada. She has appeared before all levels of Court in Canada as well as numerous administrative tribunals and arbitration panels.

alexandra.luchenko@blakes.com

Sean Boyle's practice involves all aspects of complex corporate/commercial litigation, with an emphasis on business and securities disputes. His trial and appellate experience includes contested merger transactions, take-over bids, plans of arrangements, shareholder litigation, dissent proceedings, contractual disputes, negligence claims and defending class actions. Sean has experience advising clients on compliance with domestic and international anticorruption legislation, including the Corruption of Foreign Public Officials Act. Sean also advises investment dealers on matters of regulatory compliance and has represented clients in regulatory investigations and hearings conducted by the BC Securities Commission and other provincial securities commissions, the Investment Industry Regulatory Organization of Canada (IIROC) and the Mutual Fund Dealers Association of Canada (MFDA). Sean's experience includes a secondment to the BC Securities Commission (enforcement division), where he negotiated settlements and appeared as counsel in commission hearings. Sean is active in numerous professional, academic and community organisations.

sean.boyle@blakes.com

Iris Fischer has a diverse litigation practice that includes a specialisation in white-collar crime, internal and government investigations and crisis/reputation management. She has extensive experience advising clients on domestic and foreign anti-corruption legislation, including risks of potential business practices and anti-corruption due diligence for transactions, responding to search warrants and production orders, and assisting clients with anti-corruption compliance programmes. Iris also represents clients in relation to the Competition Act, including investigations and related class actions.

As a complement to her white-collar crime practice, Iris draws on her extensive expertise litigating in the areas of media and defamation law, as well as her experience in cybersecurity, access-to-information and privacy matters to regularly advise clients in crisis. Iris has appeared as counsel at all levels of courts in Ontario, the Supreme Court of Canada and the Federal Court of Canada, as well as before administrative tribunals, arbitration panels and inquests.

iris.fischer@blakes.com

Simon Seida's practice covers various fields of commercial litigation, including class actions, professional malpractice, and post-closing disputes. In the course of his practice, he regularly appears before courts and administrative tribunals in Quebec, including for several trials. Simon also advises corporations and individuals in relation to regulatory or criminal matters, such as anti-corruption, competition or securities matters. In this context, he advises clients in responding to search warrants and investigations by government authorities or in conducting internal investigations. He also defends clients in enforcement proceedings brought by government authorities and self-regulatory organisations, including public prosecutors and securities regulators. Simon is a regular speaker on the topic of business crimes and internal investigations, and is a member of the Firm's Diversity & Inclusion Committee.

simon.seida@blakes.com

As one of Canada's top business law firms, **Blake, Cassels & Graydon LLP** provides exceptional legal services to leading businesses in Canada and around the world. We focus on building long-term relationships with clients. We do this by providing unparalleled client service and the highest standard of legal advice, always informed by the business context.

For the fifth time and fourth consecutive year, Blakes was ranked as having the leading law firm brand in the Acritas Canadian Law Firm Index. We were also named Canada Law Firm of the Year in the *Who's Who Legal Awards* for the 11th consecutive year and received the most top-tier rankings by practice area of any Canadian law firm in *Chambers Global: The World's Leading Lawyers for Business*. In addition, our lawyers continue to be recognised as leaders in their fields in *The Canadian Legal Lexpert Directory*, Canada's leading guide to lawyers.

www.blakes.com

Blakes

Cayman Islands

Angela Barkhouse
KRyS Global

One of the common themes consistent throughout offshore frauds that occur is that the assets themselves are not offshore. Fraudsters rarely leave big sums in bank accounts offshore just to earn minimal interest. They want to enjoy the fruits of their fraud, be they luxury homes, private planes, yachts, or even expensive private education.

However, the use of offshore entities to obscure the ultimate beneficial owner or fraudster is still prevalent, and the information held offshore is often critical to asset tracing and recovery.

The Cayman Islands has been referred to as a haven for fraudsters due to its perceived bank and incorporation privacy; however, the Cayman Islands' status as a leading international offshore banking and financial centre often generates actions before the Grand Court involving complex issues, financial disputes and the recovery of substantial assets for creditors or victims of fraud.

The body of legislation in the Cayman Islands is derived largely from English law, supported by English common law precedent. Thus, as in other common law jurisdictions, there are a number of legal remedies for the disclosure of information and to prevent the dissipation of assets.

However, every fraud investigation and asset recovery case has its own unique nuances, and to be an asset recovery "expert" is based on a unique understanding of which strategy or legal remedy is best suited to a particular situation. Certain situations may call for letters rogatory or the use of bilateral treaties, whilst others may call for private civil action or arbitration in a financial dispute. Insolvency mechanisms can also be used when a claimant seeks an order to appoint a provisional liquidator to secure the remaining assets for the benefit of creditors, particularly in cases where fraud or misconduct is alleged.

Recovering assets for the victims of fraud, is often vastly more complex than attempting to recover assets for a simple debt judgment, particularly where fraudsters have sought to subvert the ultimate destination of funds with the assistance of unethical facilitators. When assessing a case and a potential asset recovery strategy, it is critical to select the remedy that has the greatest opportunity to bring in recoveries. It is also important to select a team that understands the nuances of "offshore", the local jurisdiction, and is someone whom the court respects. What options are available will depend on a number of factors and it is key to ensure that you are receiving advice based on your counsel's broader knowledge and experience of asset recovery, and not, for example, based only on their expertise in recovering assets within an insolvency context. Asking for an advisor's experience in asset recovery for a wide range of fraud cases will elicit such a response.

It is to the advantage of prospective plaintiffs that the Grand Court has become adept at

leveraging the tools available to it in both criminal and civil mechanisms to permit the restraining and recovery of assets; as noted by FBI Acting Deputy Assistant Director (Criminal Investigative Division), Steven M. D'Antuono, who recently discussed before the US Senate Banking, Housing, and Urban Affairs Committee in May 2019 the "immense value" of beneficial ownership information shared by United Kingdom Overseas Territories and Crown Dependencies, including the Cayman Islands. Further, the Cayman Islands has demonstrated its capabilities in a number of high-profile civil recovery disputes, including *Ahmad Hamad Algosaibi & Brothers Company (AHAB) v Al-Sanea & Ors*, *Carlyle v. Conway*, various recovery actions for and against various feeder funds to the Ponzi scheme perpetrated by *Bernard L. Madoff Investment Securities LLC's* ("BLMIS") in 2009, the *Sphinx Group of Companies* and *Sextant Strategic Global Water Fund Offshore Ltd. et al.*

Thus, where it is believed that the perpetrators have used corporate vehicles in the Cayman Islands to conceal their proceeds of fraud, the Grand Court can be considered an advantageous forum for the application of legal remedies to assist in the tracing and recovery of stolen assets.

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

The Cayman Islands' status as a leading international offshore banking and financial centre often generates actions before the Grand Court involving complex issues and substantial assets.

The body of legislation in the Islands is derived largely from English law, supported by English common law precedent. The Grand Court is a Superior Court of Record of First Instance, having unlimited jurisdiction in both criminal and civil matters. As such, it exercises within the Cayman Islands similar jurisdiction as is vested in or capable of being exercised in England by Her Majesty's High Court of Justice and its divisional courts.

Judges of the Grand Court are appointed from amongst persons who must have the same qualifications as required for appointment to the English High Court of Justice or Courts of equivalent jurisdiction throughout the Commonwealth of Nations. In addition to the purely judicial functions, the Chief Justice is also the Central Authority for the purposes of the Mutual Legal Assistance Treaty (MLAT).

The Grand Court has a specialist Financial Services Division, which deals with cases concerning mutual funds, exempt insurance companies, financial services regulatory matters, trusts, corporate and personal insolvency, enforcement of foreign judgments and arbitral awards, and applications for evidence pursuant to letters of request from other jurisdictions.

Appeals from the Grand Court are heard in the Cayman Islands Court of Appeal, which generally sits three or four times a year. The Court of Appeal has a bench of approximately six justices of appeal, all of whom are recruited from outside the Islands and are usually sitting or retired superior court judges or justices of appeal from other Commonwealth nations. Appeals from the Court of Appeal are to the Privy Council in London.

As a common law jurisdiction, the main causes of action include the following:

- breach of contract;
- fraud;
- tort; and
- suit in equity (e.g., unjust enrichment).

Generally, the time frame imposed by the Limitation Law (1996 Revision) for bringing civil claims in tort (apart from defamation and personal injuries) and contract is six years from the date of accrual of the cause of action. Time limits may be extended in cases of fraud or deliberate concealment of the facts giving rise to a claim. As in other common law countries, it may be possible for a claimant and a defendant to mutually agree to a 'standstill', which would extend the statute of limitations. This may provide the defendant advance notice that the claimant will file a claim and therefore allow both parties an opportunity to resolve their differences without the limitations period becoming an issue.

There are no formal or mandatory pre-action steps that must be undertaken prior to the issue of proceedings, although most civil cases are commenced by the issue of a writ by the plaintiff or commenced by an originating summons.

Use of disclosure remedies

there are a number of legal remedies for the disclosure of information and to prevent the dissipation of assets.

Norwich Pharmacal order

A Norwich Pharmacal order is typically pre-action and is granted against a third party that has been innocently mixed up in wrongdoing, to force the disclosure of documents or information, which may identify another person (for example, a wrongdoer or a potential beneficiary), or to identify the nature of the wrongdoing, both of which may be the subject of subsequent legal proceedings.

To the extent the disclosure identifies additional wrongdoing by the third party, it may be possible

to use those documents, but that cannot be the purpose for which they were sought. Moreover, one can, where appropriate, apply for a 'gag order' when seeking disclosure, which directs the party not to disclose that they have been ordered to provide information to a third party. This is particularly helpful where the respondent is a bank or a professional who may have duties to give notice to their clients of such matters.

However, as in England & Wales, in order to obtain a Norwich Pharmacal order, applicants will need to show:

- that there is a 'good arguable case' that a wrongdoing has occurred;
- that the person against whom the disclosure request is sought is involved, albeit possibly innocently, in the wrongdoing as more than a mere witness;
- that the respondent is likely to have the information sought (i.e., it is not a fishing expedition); and
- that the order must be necessary and proportionate, and in the overall interests of justice.

Bankers Trust order

As the name implies, Bankers Trust orders are used to obtain information from banks. Following *Bankers Trust v Shapira* (1980) 1 WLR 1274, the court can order discovery when there is good reason to believe (e.g., as a result of tracing) that property held by the bank is, in fact, the property of the claimant and when documents produced by the bank will be used solely for the purpose of tracing money and not for any other purpose. It does require that the claimant gives an undertaking in damages, and the claimant to undertake to pay any and all expenses resulting from the bank giving discovery.

Interim relief

Interim relief to prevent the dissipation of assets by, and to obtain information from, those suspected of involvement in the fraud are available through Mareva injunctions (freezing orders) to prevent dissipation of assets and Anton Piller orders.

Mareva injunction

Mareva injunctions freeze the assets of a party pending further order or a final resolution of the court. To the extent the respondent is in a common law jurisdiction and he or she seeks to move or transfer assets without approval of the court, he or she can be found in contempt and, in some extreme cases, be denied the ability to provide a defence until he or she complies.

In addition, a Mareva injunction will normally compel an accounting from the respondent of his or her assets. However, the court can require that the party applying for the order provide security or a bond, also known as a cross-undertaking. The rationale for this is that because it is such a draconian remedy, if the claim is not successful then the respondent may be entitled to damages for financial or reputational loss caused by having the injunction placed upon him or her.

Anton Piller order

An Anton Piller order can be obtained providing the right to search premises and seize evidence that is the subject matter of the dispute *ex-parte* (without warning the defendant). It can prevent the destruction of relevant evidence, and is particularly useful in ensuring electronic evidence on computers or mobile devices is preserved. In order to obtain an Anton Piller order, the following must be demonstrated:

- that there is *prima facie* evidence of the wrongdoing;
- that the potential or actual damage is very serious;
- that there is clear evidence that the respondent has incriminating evidence in his or her possession; and
- that there is a real possibility the respondent may destroy this material if he or she were to become aware of the application.

Insolvency

The use of insolvency processes and/or the court appointment of a receiver (particularly in jurisdictions that follow common law) can be particularly advantageous in investigating cases of fraud, corruption or misappropriation of assets. Whilst perhaps not foremost in the minds of many, it is a tried and tested method, and is appropriate for both insolvent and solvent companies. As in the case of a solvent company, it would be considered in the public interest for the company in question to be wound up, having been complicit in, or used as a vehicle for, fraudulent misconduct. In addition, as a stakeholder in the liquidation, fraud victims have a greater level of insight into the investigation and strategy being employed.

Thus, if a fraud has been perpetrated, the applicant or victim can seek to have a company wound up on a "just and equitable basis" by the court, particularly if it believes that it is necessary to prevent the dissipation or misuse of the company's assets. Once a liquidator is appointed, he can secure the remaining assets for the benefit of creditors and commence an investigation into the circumstances of the fraud. Often an application for a just and equitable winding up can be made *ex-parte*. Such an application is often used to avoid any "tip off" to the fraudsters which can lead to the further dissipation of assets, and has

been used in the Cayman Islands for a number of high-profile cases.

Insolvency proceedings begin by petition. It is the plaintiff's (or petitioner's) responsibility to serve the other parties with the originating process once it has been issued by the court office. Within insolvency mechanisms a useful cause of action available to a liquidator, under statute and with the authority of the court, is the ability to challenge transactions that have not benefited the company, such as unfair preference claims (e.g., gifts or transactions to related parties), wrongful or fraudulent trading and transactions at undervalue; these remedies are only available within the context of a liquidation.

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

In assessing a case and the asset recovery strategy, it is critical to select the remedy that has the greatest opportunity to bring in recoveries. Litigation is not a guarantee of asset recovery, even with a successful judgment; however, working in conjunction with legal counsel is critical for reasons of privilege and to ensure proper legal advice is received regarding the strategy. What options are available will depend on a number of factors:

1. What information is already available, and which may help in finding further information. For example, are you looking for information to assist with proving the fraud, information on assets, to depose a potential witness/target, pursue an asset or potentially litigate against another party?
2. Where do the fraudsters reside or operate? Where do they spend their time? How do they live?

   The more information is available about the fraudster the easier it is to identify what may be the easiest assets to recover initially, and therefore the potential targets for information and assets.
3. What jurisdictions are you considering, and in particular whether they are civil law or common law?

There is often a logical order to pursuing assets, as evidence from one jurisdiction may be necessary to provide evidence to pursue an asset in another jurisdiction. There may be certain local legislation or nuances that legal counsel will need to navigate.

Whilst each fraud investigation and asset recovery assignment will be unique in what information and documentation is available, ideally the first port of call is the marshalling preserving and documenting of any evidence that does exist, including all email, electronic and financial data. A review of emails and working documents through key word searches on an e-discovery platform may reveal intentional conduct, consciousness of guilt, plans to defraud or unknown businesses or shell companies. Examination of financial data will help determine the flow and destination of funds and therefore assets, using proprietary data analytical tools to identify outliers and anomalies.

Sometimes the starting point will be based on an investigation of publicly available information only. Depending on the jurisdictions identified we will undertake research into various information databases, such as corporate registries, litigation filings, and also review online information such as media reports, and social media profiles.

Triangulating client documentation, open source intelligence with corporate records and available publicly held documentation may reveal

related party transactions and the ultimate destination of funds. The findings in this phase will assist the team in developing a strategy for further investigation.

Once exhausted and at the appropriate juncture we may turn to appropriate discovery tools such as a Norwich Pharmacal order or Bankers Trust order (as referred to above), to get behind the wall of shell entities we have been unable to penetrate or to obtain additional information on the flow of funds. With sufficient investigative work, the next stage will normally be the service of the claim.

Parallel proceedings: a combined civil and criminal approach

Parallel proceedings in civil and criminal matters that are based on the same set of facts are permissible; however, a court may stay a civil proceeding if a defendant would be unjustly prejudiced by providing information in said proceeding that may incriminate him or her in future or current criminal proceedings.

Of instructive authority is the case of *Panton v Financial Institutions Services Limited* [2003] UKPC 8, in which the Privy Council concluded that in order to obtain a stay of parallel civil proceedings, the defendant would have to show that he or she would suffer unjust prejudice in the ongoing criminal proceedings if they were to continue, taking into account competing considerations between the parties.

The burden of proof (should there be a stay in proceedings) will lie with the defendant, who must point to a real and non-notional risk of injustice: 'A stay would not be granted if it was deemed to be simply to obtain a tactical advantage by a defendant in criminal proceedings.'

The Director of Public Prosecutions is the only person formally entitled to bring criminal asset recovery proceedings and, as such, private prosecutions or class action suits are not available in the Cayman Islands.

Key challenges

A challenge for victims of fraud is the ever increasing costs of funding a claim, particularly for victims who have lost significant, and life-changing sums. Whilst in recent years there has been an increase in litigation funding to assist in bringing a claim to fruition, in the Cayman Islands, traditionally, the Grand Court has restricted funding for insolvent liquidation estates; Liquidators have a statutory power to sell the 'fruits of an action' to a third-party funder, subject to the approval of the court.

Although the doctrines of maintenance and

champerty have yet to be formally abolished in the Cayman Islands, the court in *A Company v A Funder* (November 2017), being mindful of the law of maintenance and champerty in other common law jurisdictions, concluded that overall, a proposed funding agreement was legitimate on the basis that "*it did not corrupt public justice, undermine the integrity of the litigation process and give rise to a risk of abuse*" (J Segal). The court will consider, in particular, the relationship between the funder and the claimant, and the ability of the funder to control or interfere with litigation strategy.

In my personal view, I would like to see it more readily available for third-party funders to assist in bringing claims, which would otherwise not see the light of day due to the financial constraints of fraud victims. The financial impact of fraud does not just apply to individuals, but to entities too; fraud can have debilitating effects on a company; on its profits, consumer confidence, and in severe cases its reputation and the cutting of its workforce or its entire collapse. Allowing fraudsters to enjoy the spoils of their illicit gains whilst innocent victims are left to deal with the devastating repercussions cannot be a just or equitable outcome.

Cross-jurisdictional mechanisms: issues and solutions in recent times

The Grand Court recognises the need to respect and cooperate with judges in other jurisdictions and commands similar respect in return. As a result, cross-border asset recovery in the Cayman Islands, particularly when dealing with other common law jurisdictions should not faze a victim if considering whether to pursue stolen

assets. However, some caution may be necessary if the need to recognise orders or deal with civil law countries arises.

Both the Grand Court and the Court of Appeal have referred to the well-known English decision in *Rio Tinto Zinc Corp. v Westinghouse*, in which the English court observed that *"it is the duty and pleasure of the English court to do all it can to assist the foreign court, just as the English court would expect the foreign court to help it in like circumstances"*. Indeed, the Grand Court has consistently adopted that approach. High-profile examples of cross-border cooperation include the case of *Bank of Credit and Commerce International (BCCI), Ahmad Hamad Algosaibi & Brothers Company (AHAB) v Al-Sanea & Ors, Carlyle v. Conway*, various feeder funds to the Ponzi scheme perpetrated by *Bernard L. Madoff Investment Securities LLC's* ("BLMIS") in 2009, the *Sphinx Group of Companies* (with investor claims exceeding US$730 million and assets in the estate amounting to US$530 million) and *Sextant Strategic Global Water Fund Offshore Ltd. et al.*

The Grand Court can also use any of the common law tools to order the disclosure of documents for use in proceedings in another jurisdiction to assist with asset preservation and evidence gathering, including those referred to above: Norwich Pharmacal and Bankers Trust orders, Mareva injunctions and Anton Piller orders. Although it should be noted that a "person" cannot be compelled to give any evidence under an order that they would not have been compelled to give in civil proceedings in the Cayman Islands or in the country where the requesting court exercises its jurisdiction.

Information can also be obtained through courts in other jurisdictions under The Hague Convention on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters 1965 and The Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters 1970 subject to their being a contracting state party.

When dealing with criminal matters, whether in support of matters overseas or originating from the Cayman Islands, the main avenue for provision of assistance by the Cayman Islands is the Under the Criminal Justice (International Cooperation) Law (2015 Revision) (CJICL). When assisting in investigative matters from other countries, mutual legal assistance is to be provided at the investigative stage of a matter where the conduct would constitute an offence in the Cayman Islands. The registration or enforcement of confiscation orders made by courts of other jurisdictions is governed by the Proceeds of Crime Law (2019 Revision) (PCL). The Cayman Islands can also implement legal tools provided within any of the United Nations conventions or other international treaties to which it is party. Although dual criminality is generally a requirement in all cases, technical differences in the categorisation of offences should not pose an impediment to mutual legal assistance.

The Cayman Islands is also party to the Asset Recovery Inter-Agency Network for the Caribbean (ARIN-CARIB), launched in 2017 to establish a network of contact points in the region and focus on all aspects of asset recovery activities and assistance. The network is an informal cooperative group used among member countries for the expedient sharing of information, and use of multiple tools to trace, freeze or seize assets of an international criminal organisation. This can be useful for the process of asset recovery in providing information that can be used in a formal mutual legal assistance or letter rogatory process.

The Evidence (Proceedings in Other Jurisdictions) (Cayman Islands) Order 1978 (EPOJ) enables the Grand Court to provide assistance to foreign courts in obtaining evidence in both criminal and civil cases. Requests are made through letters rogatory and can be requested by any country. As a successful example of a matter involving letters rogatory, the Cayman authorities acted proactively in the matter of Vladimiro Montesinos, the former chief of intelligence and main advisor of former Peruvian President Alberto Fujimori, and who is serving multiple sentences for human rights crimes, corruption and arms and drugs trafficking. Former president Alberto Fujimori is himself serving a 25-year sentence for corruption and authorising death squad killings (Published on – StAR Stolen Asset Recovery Initiative – Asset Recovery Watch

(2017)). The authorities took "*recourse to restrain the money itself in rem out of concern that the local laws were also being violated, instead of awaiting a judgment in personam which may never have been forthcoming because of the fugitive status of the perpetrator and which would have to be also enforced to recover the proceeds which would have no doubt taken flight within the restraint*". This action resulted in the repatriation of some $44 million dollars to Peru, without a trial between the parties having to take place (see the Cayman Islands Government webpage on Enforcement of Judgments in Practice).

Finally, in relation to cases which have utilised the insolvency mechanism for asset recovery, the Chief Justice in May 2018 issued a new Practice Direction to strengthen court-to-court cooperation in cross-border insolvency and restructuring cases, being the guidelines adopted in the American Law Institute/International Insolvency Institute Guidelines Applicable to Court-to-Court Communications in Cross-Border Cases and the Judicial Insolvency Network Guidelines for Communication and Cooperation between Courts in Cross-Border Insolvency Matters. Whilst the Cayman Islands has not adopted the UNCITRAL Model Law, it should be noted further work is being undertaken by UNCITRAL to improve the recognition of asset tracing and recovery mechanisms between common and civil law jurisdictions, which may be beneficial for awards obtained in the Cayman Islands (https://uncitral.un.org/en/assettracing, an invitation only event for experts to: (a) examine both criminal and civil law tracing and recovery with a view to better delineating the topic while benefitting from available tools; (b) consider tools developed for insolvency law and for other areas of law; and (c) discuss proposed asset tracing and recovery tools and other international instruments. This author was one of the experts invited to participate).

Technological advancements and their influence on fraud, asset tracing and recovery

Investigative technology continues to improve with the advancement of automated and machine learning software, innovative use of algorithms to identify anomalies, outliers and previously difficult to obtain information, and the improvement of document management systems and e-discovery platforms; all of which assist the investigation teams to analyse massive amounts of structure and unstructured data which can be presented to end users and, in particular, the court in a robust and defensible way.

Specifically, to the Grand Court, it has video conferencing equipment in many of its court rooms to enable, in appropriate circumstances, the cross-examination of foreign witnesses and hearings to be conducted by advocates in different time zones. This was particularly demonstrated in the case of *Ahmad Hamad Algosaibi & Brothers Company v Saad Investment Company Limited and Others,* in which a 129-day trial was conducted. During the trial, software allowed for a live audio feed and a real-time transcript that was simultaneously accessible around the world. In court, the legal team and the judge had access to electronic trial bundles with 'personalised' versions of marked up documents displaying evidence which included over 250,000 documents for consideration.

The Cayman Islands has recently developed as a jurisdiction of choice for companies conducting token generation events or ICOs (Initial Coin Offerings) including the largest ever ICO to have taken place in 2018, with USD$4.1 billion raised. Whilst no specific legislation has been passed by the Cayman Islands Government as yet, the Ministry of Financial Services warns that "*persons engaged in virtual asset services in or from within the Islands are therefore reminded that they are subject to, and are required to comply fully with, the provisions of the AMLRs and all other applicable laws".*

As such, any case of fraud relating to an ICO, token sales, token exchanges, that took place in the Cayman Islands, would be subject to the current regulatory and legal framework as per the below:

- The Monetary Authority Law.
- The Securities Investment Business Law.
- The Proceeds of Crime Law.
- Anti-Money Laundering Regulations.
- The Mutual Funds Law.
- The Electronic Transactions Law.

In addition, recent FATF recommendations regarding the regulation and supervision of virtual assets and the provision of virtual asset services urge countries and obliged entities to comply with its recommendations to prevent misuse of virtual assets (VAs) for ML and terrorist financing; the Cayman Islands is a member of the Caribbean Financial Action Task Force (CFATF).

However, some key challenges with dealing with cryptocurrency frauds, in particular the use of "mixers" to launder money remain; although it should be noted that those challenges are not limited to the Cayman Islands. For example, "mixers" which are used to try to prevent such tracing, by making it difficult or impossible to identify the source of a transaction, can obfuscate the tracing of funds. The basic premise of a mixer is the pooling of cryptocurrency, and then taking back coins of the same value but which will have originated from a different source (or sources) than the ones they brought to the mixer. Ultimately, users are relying on the mixer service or exchange not to disclose the source of each bitcoin or any information about its users. Currently, it is estimated that around $2.5 billion has been laundered through cryptocurrency from proceeds of crime, although that is dwarfed by the approximately $1 trillion per year is laundered in fiat currency (Bitcoin Money Laundering Statistics (2020 Updated)).

Recent developments and other impacting factors

In the case of *Ahmad Hamad Algosaibi & Brothers (AHAB) v Saad Investment Finance Corporation Ltd and Others*, 2018, the Grand Court held that although the law may infer necessary transactional links to give rise to a tracing claim where there is a scheme 'specifically designed' to subvert the ability of creditors to recover misappropriated funds, the general rule remains that it is necessary to establish a chain of transactions to trace funds.

The Court then went on to make a number of other important observations for the law of tracing, in particular with regard to jurisdiction where it held that given the alleged misappropriations took place in Saudi Arabia, the proper law governing AHAB's equitable claims was Saudi law. As Saudi law does not recognise a proprietary remedy in these circumstances, it was not possible for AHAB to establish a proprietary base on which to establish its tracing claim.

Thus, dealing with a lack of appropriate legislation in the originating country may be an issue with asset tracing claims. As such, careful consideration of a basis for a tracing claim will need to be considered.

Director Registry

Other impacting factors include the introduction of new legislation in the Cayman Islands, which grants any person the ability to inspect a new 'list of names' of the current directors of a Cayman Islands company and a list of names of the current managers of a Cayman limited liability company upon payment of a fee. Any inspection must be at the offices of the Registrar in person and will be subject to such conditions as the Registrar may impose.

Ultimate Beneficial Ownership Register

Most of the British Overseas Territories have announced their intention to introduce a public register of beneficial ownership once the European Union countries establish their own public registers. In the interim, service providers in the offshore jurisdictions are updating their current records and in some jurisdictions, there is a new requirement (for instance the Cayman Islands) that the register of members specify, with respect to each category of shares, whether such category of shares carries voting rights and, if so, whether such voting rights are conditional.

Economic Substance Law

The Cayman Islands, along with most other British Overseas Territories have also brought in legislation that requires certain entities incorporated in those jurisdictions to have demonstrable economic substance in those jurisdictions. "Relevant entities" that carry on activities offshore must satisfy an economic substance test. This can include evidence that it is conducting

core income-generating activities on the Islands, that it is directed and managed in an appropriate manner on the Islands, and that having regard to its economic activity.

The legislation and guidance is yet untested and many incorporated entities are entering contracts with service providers to rent office space, retain accounting records, hold annual general meetings and carry out other local activity to address these new requirements. To the extent discovery is being considered, these requirements may provide other options for collecting relevant and useful information on the entity's operations and who controls the entity's business affairs.

The above developments in the legislation of the offshore jurisdictions means there is or will be in the future further opportunities for collecting information and relevant documents in the investigation of fraud and illicit activity. There is, however, a negative consequence of the above. We have observed various entities winding up their entities in the British Overseas Territories as owners and management consider other means to conceal or at least not make so readily available the details of directors and beneficial owners of a company. The explanation for many of these closures is cost, but it could perhaps be more sinister than that.

Angela Barkhouse is a financial crime investigator and international asset recovery practitioner with a diverse range of clients in banking, government, HNWI's, law firms and corporations. With 15 years of professional experience, Angela has investigated bribery, corruption, malfeasance, conflicts of interest, embezzlement, stolen wealth, identified stolen assets, and made cross-border asset recoveries utilising a range of asset recovery tools in support of criminal and civil litigation.

Angela has also acted as an independent expert upon international projects in anti-corruption and asset recovery, (for example on behalf of the UNDP in Tunisia) and contributes to articles and policy papers on the same. She is recognised as an expert in asset recovery by *Who's Who Legal 2019* as "tenacious" and "fearless", and for her "imaginative and innovative investigative strategies". Angela is a Fellow of the Association of Certified Chartered Accountants, a Certified Fraud Examiner and Insolvency Practitioner, and holds degrees in Applied Accounting (BSc) and Criminal Justice Policy (MSc).

angela.barkhouse@krys-global.com

England & Wales

Keith Oliver
Peters & Peters

Amalia Neenan
Peters & Peters

Fraud is a major risk to the global economy. The threat level is particularly high in the UK, with £1.2 billion being stolen as the product of fraud in 2018. Although admirable efforts have been made to recover these funds, the ratio of recovered assets to lost is exorbitantly skewed in favour of the latter. 2020 is set to be an important year for the legal sector, with key impacting factors such as Brexit, and the ever rapidly evolving nature of technology, affecting both our domestic legal instruments and our place in the international community.

In relation to fraud and asset tracing, these factors simultaneously create opportunities for disruption and innovation. Therefore, in this chapter we explore the current legal framework underpinning fraud, asset tracing and recovery cases in England & Wales, examining what the mechanism of tomorrow may look like.

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

> *'Tremble, thou wretch, that hast within thee undivulgèd crimes, unwhipped of justice.'*
> King Lear
> Act III, Scene III

It would be whimsical to think that Shakespeare's immortal words in *King Lear* were really an allegory for the guiding principles that steer the courts of England & Wales. Though perhaps not his intention, the Bard's insight seamlessly transfers into the fraud arena as a warning: those with *'undivulgèd crimes, unwhipped of justice'* should tremble, as the courts will come after you. The English courts warrant this reputation. The unparalleled impartiality and extensive range of technical expertise of the judiciary is admired the world over. So much so, that even with the uncertainty of Brexit and another general election in 2019, the London Commercial Court has never been busier. The Portland Litigation Consulting 2019 report indicates that there was a 63% increase of cases heard from the previous year, with non-UK litigants accounting for 60% of users. Moreover, there was a 45% increase in civil fraud cases from 2018, making it the third most common type of litigation, behind arbitration challenges and contractual disputes.

This is unsurprising, as it was the English legal system that essentially launched the global methodology employed in fraud and asset recovery that we use today. For instance, the English courts are well known for their development of unique and powerful orders for relief. Anton Piller orders were one such tool

that was instrumental in sculpting the fraud recovery landscape worldwide. Derived from *Anton Piller KG v Manufacturing Processes Limited* CA 8 Dec 1975, these orders allow for the search and seizure of evidence if, as per Ormrod LJ, *'first, there must be an extremely strong prima facie case. Secondly, the damage, potential or actual, must be very serious for the applicant. Thirdly, there must be clear evidence that the defendants have in their possession incriminating documents or things, and that there is a real possibility that they may destroy such material before any application inter partes can be made'*. This then gave way to the statutory search order enshrined in section 7 of the Civil Procedure Act 1997, but not before the model established at the common law had been adopted by a plethora of different jurisdictions. Hong Kong and South Africa are but to name two.

The same can be said of Mareva orders. This freezing order was borne from the case *Mareva Compania Naviera SA v. International Bulkcarriers SA*, [1975] 2 Lloyd's Rep 509, and was an order deployed to prohibit judgment debtors from frustrating judgments against them by dissipating their assets. Similarly, these powers are now codified under section 37(1)&(3) of the Senior Courts Act 1981, and in Practice Direction 25A of the Civil Procedure Rules 1998. However, the original Mareva model has been adapted in some form or another internationally. In conjunction with this, the English system has another ace up his sleeve when it comes to utilising freezing orders on a global scale. Under section 25 of the Civil Jurisdiction and Judgments Act 1982, the English High Court has the ability to grant freezing injunctions to assist proceedings in a foreign country, as long as doing so would not be inexpedient, is ancillary to the foreign proceedings and, in the case of intra-EU litigation, that there is a real and connecting link between the specified assets and England. This powerful international tool sets the UK apart in that this long-arm jurisdictional reach sends a powerful message to fraudsters. Wherever they run, the English courts will be in pursuit.

Another key mechanism is the Proceeds of Crime Act 2002 (POCA). Part 5 of POCA is intended to be used to enable *'the enforcement authority to recover, in civil proceedings before the High Court… property which is…obtained through unlawful conduct'* (section 240 (1)(a)). Unlawful conduct is defined as conduct which occurs *'in any part of the United Kingdom…if it is unlawful under the criminal law of that part.'* (section 241 (1)). Part 5 also extends this provision to capture conduct *'which occurs in a country or territory outside the United Kingdom and is unlawful under the criminal law applying in that country or territory, and …if it occurred in a part of the United Kingdom, would be unlawful under the criminal law of that part'* (sections 241(2)(a) & (b)). The broad nature of Part 5 is demonstrated in section 242(2)(b), which does not impose restrictions of the type of conduct necessary to be counted as unlawful. *'It is not necessary to show that the conduct was of a particular kind if it is shown that the property was obtained through conduct of one of a number of kinds, each of which would have been unlawful conduct.'*

However, the scope of POCA does not end here. Instead, it also provides for key court orders that can be deployed on a without notice basis during the course of an investigation. One of the most powerful tools is a section 357 disclosure order. *'A disclosure order is an order authorising an appropriate officer to give to any person the appropriate officer considers has relevant information notice in writing requiring him to do, with respect to any matter relevant to the investigation for the purposes of which the order is sought, any or all of the following— (a) answer questions, either at a time specified in the notice or at once, at a place so specified; (b) provide information specified in the notice, by a time and in a manner so specified; (c) produce documents, or documents of a description, specified in the notice, either at or by a time so specified or at once, and in a manner so specified.'*

Nevertheless, despite this order's wide-reaching effect, there are specific safety-net requirements that must first be met before it can be issued. For example, there must be reasonable grounds for suspecting that *'the person specified in the application for the order holds recoverable property or associated property'*, that the order be in the public interest, and *'information which may be provided…is likely to be of substantial value (whether or not by itself) to the investigation for the purposes of which the order is sought'* (Section 358(2)(3)).

POCA is therefore a vital instrument in the war on fraud. Importantly, this is not a *'static'* statute, it is receptive to change to combat the ever-evolving threat of fraud head on. Most recently, this was exemplified in the creation of Unexplained Wealth Orders (UWOs). UWOs are civil orders that shift the burden of proof by requiring individuals, who are either Politically Exposed Persons not in the EEA or suspected of involvement in serious crime, to explain how they obtained a particular property/asset (that is of a value in excess of £50,000), if it is reasonably believed that their legitimate known income would have been insufficient to finance those acquisitions (section 362A (3) POCA). It is important to note that UWOs are investigative powers only, and it is not *'(by itself) a power to recover assets. It is an addition to a number of powers already available in POCA to investigate and recover the proceeds of crime and should therefore not be viewed in isolation'*. (Home Office, *'Circular 003/2018: unexplained wealth orders'*, 1 February 2018.)

UWOs are a reactionary tool created in the wake of the March 2016 Transparency International UK report entitled *'Empowering the UK to Recover Corrupt Assets: Unexplained Wealth Orders and Other New Approaches to Illicit Enrichment and Asset Recovery'*. This publication was a catalyst in the reinvigoration of UK legislation designed to combat financial criminality. At the time, the report concluded that the existing legislative controls had allowed *'a large amount of corrupt wealth, stolen from around the world'* to be invested in the UK. The campaign group contended that the methods of asset recovery currently available were *'not fit for purpose...* [and] *undeniably very limited compared to the scale of the threat'*. (Transparency International UK, *'Empowering the UK to Recover Corrupt Assets: Unexplained Wealth Orders and other new approaches to illicit enrichment and asset recovery'*, March 2016.) Following this report, the Government released the *'Action Plan for Anti-Money Laundering and Counter Terrorist Finance* (Home Office, *'Action Plan for anti-money laundering and counter-terrorist finance,' April 2016*), in an attempt to remedy the prominent risk-areas under the then statutory framework. The legislative proposals of the Action Plan were then encapsulated in The Criminal Finances Act 2017. Sections 1–6 of The Criminal Finances Act 2017 introduced sections 362A–362R and 396A–396U into Chapter 2, Part 8 of POCA, which is the statutory backing for the UWO regime.

The first UK UWOs were obtained on 28th February 2018 in *National Crime Agency v A [2018] EWHC 2534 (Admin)*. The case was shrouded in mystery as identification restrictions resulted in the identity of the respondent remaining sealed for a significant proportion of the case, using the alias *'Mrs. A'*. It was then revealed that she was Zamira Hajiyeva, the wife of a disgraced Azari banker, and that the orders related to £22 million worth of property that she owned in the UK. The UWOs required her to explain how she could fund her lavish lifestyle, which saw her spend £16 million in Harrods over a decade, and the aforementioned properties. She sought to challenge the characterisation of her husband as a PEP. The appeal judgment at the time of writing has been reserved. Regardless of the outcome, these powers are just the tip of the iceberg when it comes to the UK's resolve to stamp out fraud and ensure a robust and effective asset retrieval system.

II Case triage: Main stages of fraud, asset tracing and recovery cases

Whilst the scope of this chapter is exclusively civil, criminal sanctions can be considered in conjunction with civil asset recovery if parallel proceedings are in play. For a more detailed exploration of parallel proceedings, please see Subsection III. Moreover, a symbiotic and complimentary approach, utilising both civil and criminal legal powers should be considered throughout the process, to advance effective recovery practices.

When approaching civil fraud cases, it is generally accepted that there are four main stages to asset recovery: 1) *Triage/Preliminary Case Assessment*; 2) *Evidence Gathering*; 3) *Securing*

the Assets & Evidence; and 4) *Enforcement & Confiscation*.

The first stage, *Triage/Preliminary Case Assessment*, is an initial assessment to fact find and gather intelligence, as well as establish an investigation and tracing strategy. Part of this strategy planning will include identifying a preferred jurisdiction. Due to the wealth of court powers available under the civil system, England & Wales is an ideal jurisdiction. To illustrate, the High Court not only has jurisdiction over any defendant domiciled in England & Wales, but also over non-domiciled defendants under EU Regulation 1215/2012 on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters (Brussels 1 Regulation (Recast)), individual jurisdiction agreements or through the Common Law. Therefore, defendants can be sued in a State where they are not domiciled, if it can be demonstrated that another jurisdiction is more appropriate. It is also appropriate to determine the availability of third-party funding. Third-party litigation funding (TPLF) is a burgeoning area, particularly in civil fraud and asset recovery cases. In 2017, Global funding enterprises that operate in the UK raised over $10 billion in litigation financing (Thompson, B., '*Lawsuit funders raise $10bn from yield-hungry investors*', The Financial Times, November 2017). TPLF works through investors financing legal disputes in return for a percentage of any damages won. This can help to level the playing field, giving under-resourced claimants greater access to justice.

The second stage, *Evidence Gathering*, is essential and it is here that civil and criminal powers may complement each other. Without the proper gathering of the full spectrum of available and admissible evidence, a meritorious case may encounter difficulties at the first hurdle. This process may involve working with forensic IT experts/accountants and regulatory agencies. It can, and most likely will, require obtaining information from third parties (which may necessitate a range of civil disclosure orders, such as Norwich Pharmacal relief against banks or financial institutions). Finally, this may include collecting evidence from offshore jurisdictions. This can be difficult if the jurisdiction in question has a lax attitude towards preventing fraud, and so may be reluctant to share information. Therefore, it might be fruitful to deploy criminal powers in some instances to aid civil recovery. For instance, evidence can be gathered in multiple jurisdictions using domestic criminal powers or Mutual Legal Assistance, which can then be used in civil proceedings. For a further discussion on this aspect, see Subsection V.

Stage three, *Securing the Assets & Evidence*, uses the plethora of the UK courts' interim orders to protect evidence and assets that may become subject to litigation and enforcement. Take for example search orders. They allow for the defendant's premises to be entered to identify and preserve evidence relevant to the action. Moreover, worldwide freezing orders prevent defendants from dealing with any of their assets above a certain monetary level anywhere in the world. Tracing orders require defendants to set out in an affidavit their dealings with specific assets or monies over which the claimant asserts a proprietary right. Passport orders may be obtained in respect of defendants who pose a risk of flight from the jurisdiction. Finally, in certain cases, it may be possible to appoint a receiver to take control over the defendant's assets and manage them pending the determination of any claim.

Stage four, *Enforcement & Confiscation*, is contingent on the effective implementation of the first three stages. This will then ensure that appropriate remedies from the available suite of legal solutions are pursued, to successfully enforce a judgment against a fraudster for the confiscation and repatriation of stolen assets. A further discussion on enforcement mechanisms is found in Subsections V and VII.

III Parallel proceedings: A combined civil and criminal approach

In most scenarios, there is nothing to prohibit the use of parallel criminal and civil proceedings

in this jurisdiction. The only caveat to this is when there is a real risk that the defendant would be subject to severe prejudice in either the criminal or civil proceedings, or both. This would be the case if there was sufficiently negative media coverage or publicity that has been caused by the simultaneous running of both cases. Notwithstanding these difficulties, the advantages of a multi-pronged attack can be a fruitful. The shortfalls of one system can be addressed by the other. For example, punishment of offenders is the overriding objective of the criminal justice system. However, although this may be a consideration for victims, ultimately, most parties are concerned with the retrieval of their stolen funds, which is why the civil mechanism is vital. Nevertheless, practitioners must be aware of the potential pitfalls that can occur when evidence or information is gathered through the investigation of one set of proceedings and whether, if at all, it can be used in the other. Moreover, Defendants can employ stalling tactics by using the excuse that there are simultaneous proceedings in play. For instance, this could be to seek a delay in complying with court orders until the outcome of the other case. Yet, conglomerating these tools allows for an all-encompassing attack on fraudsters, assisting in making victims whole again.

However, despite the best efforts of a combined approach, in some instances neither a traditional criminal prosecution nor a civil litigation may be viable. Due to a variety of factors, the most prevalent of which is usually a lack of funding, it is increasingly common to find that the police or the CPS refuse to investigate or bring certain cases to trial. In 2017, only 3.1% of fraud cases were solved by local police, with 12.1% classified as *'ongoing'*, leaving 85% unsolved. Furthermore, even though the civil route may be able to pick up the slack in these circumstances, the process is still arduous in terms of both the length of procedure and the expense involved in bringing a civil claim.

Subsequently, there has been an increase in the utilisation of private prosecutions. In *R v Zinga [2014] EWCA Crim 52*, the Lord Chief Justice submitted that *'at a time when the retrenchment of the State is evident…it seems inevitable that the number of private prosecutions will increase'*. An individual or a company who has been defrauded can bring a private prosecution under section 6(1) Prosecution of Offenders Act 1985. Proceedings will take place in the same manner as if they were brought by the Crown and are normally held in the Magistrates' Court in a matter of weeks. Typical timeframes on these types of cases, depending on the evidence involved and whether funds or criminality have a foreign jurisdictional nexus, can take up to nine months to complete, which although substantial, can be faster than both the normal criminal and civil avenues. Other benefits to this mechanism include greater control for victims in deciding how the case progresses. For example, victims can decide what compensation orders should be sought, the proceeds of which will go to the victim, unlike public prosecutions where confiscated assets are given to the State.

The largest private prosecution in the UK to date was the 2018 successful conviction of Paul Sultana. Sultana had defrauded the off-shore engineering company Allseas out of £88 million, and consequently was jailed for eight years in private proceedings after the Crown Prosecution Service had originally refused to charge him. Therefore, whether a symbiotic criminal and civil approach is taken, or a private prosecution is brought, it is clear to see that the courts of England & Wales are eager to offer redress for victims in a glut of inventive ways, sending the message that there is nowhere for fraudsters to hide in this jurisdiction.

IV Key challenges

The process of investigating fraud and attempting to retrieve misappropriated funds can be hindered by different challenges. As with most things, information is key. In order to effectively trace assets, extensive information gathering expeditions are made in order to secure leads on where assets may have been transferred (see Subsection II). This may be as simple as

searching a public database, to more nuanced investigative tools such as seeking court orders to collate the requisite information. However, this may not be as simple as it sounds. It takes time and resources to collect such information.

Additionally, in the digital era, two scenarios commonly occur. The first is where technological advancements have created information *'blackholes'*, allowing fraudsters to hide behind levels of encryption to mask their identities when stealing assets. Data deficits can create severe hinderances to both the prosecution of fraudulent actors, and the retrieval of the monies they have taken. Scenario two looks at the opposite end of the spectrum, when there is an abundance of data that must be analysed, converted into a usable format and then interpreted. This is exceedingly time and resource intensive, requiring specialist knowledge and expertise.

However, one of the biggest challenges practitioners face is the constraints that arise with cross-border asset recovery. The next Subsection deals with this particular obstacle in more detail.

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

Today, fraud, asset tracing and recovery cases are rarely domestic in their entirety. Misappropriated assets are often hidden across national borders and require international cooperation to be traced effectively. Nevertheless, different jurisdictions take different approaches to tracing and recovering assets. Differing legal procedures, or attitudes to fraud, can complicate the cross-border coordination of recovery. For example, off-shore jurisdictions, like the BVI, are known as havens for illicit monies. This is in part due to secrecy provisions that cover the true identities of beneficial ownership. Although some Crown dependencies, such as Jersey, Guernsey and the Isle of Man, have vowed to introduce completely public ownership registers by 2023, there is a surfeit of jurisdictions that avoid these provisions, blocking asset tracing. Therefore, the courts of England & Wales have had to creatively circumvent these obstacles.

One of the main ways is through the smooth enforcement of English judgments overseas. Within the European Union, the Brussels 1 Regulation (Recast) allows for the relatively easy enforcement of judgments within each Member State. In the run up to Brexit, it will remain to be seen what tool will supplant this mechanism. For a more in-depth discussion on this tool, please see Subsection VII. Regardless of the Brexit outcome, there are already systems in place that help when it comes to dealing with jurisdictions outside of the European Union. Fraud is truly a global crime and does not limit itself to one geographical or economic trading block. Therefore, the UK is incredibly adept at pursuing fraudsters and their loots internationally.

English judgments are widely recognised and enforced in many jurisdictions, with systems that, much like the English regime, allow for the deployment of legal weapons that can ensure judgment creditors get their due. For example, one of the key considerations of international asset tracing is that once the monies are located, they must stay put. Therefore, English courts use tools such as worldwide freezing orders that can block the transfer of any funds or assets in the possession of the fraudster, which can ensure both the successful enforcement of an English judgment overseas, and the ultimate retrieval of funds that have found themselves there.

VI Technological advancements and their influence on fraud, asset tracing and recovery

The March of Technology has raced forward with great momentum over the past few years, drastically altering the legal landscape in its wake. The civil fraud and asset recovery sphere is but one sector that has experienced a sort of *'whiplash'*, as advancements in technology present progressive challenges to the curtailment of fraud.

As a result, a slew of new methodologies for deception have become the *tools du jour* for the

cyber-age fraudster. Take, for example, the use of *'Deepfakes'*. Deepfakes are technology that allows footage or audio recording of an individual to be replaced with another person's likeness. The malicious use of this technology has led to new avenues for fraud. Audio Deepfakes have been used to con people into parting with money through telephone conversations which the victim believes are from a legitimate source. In 2019, Forbes reported that the CEO of a UK-based energy firm had been duped into transferring $243,000 to a fraudster using an Audio Deepfake of the CEO's superior (Jesse Damiani, '*A voice Deepfake was used to scam a CEO out of $243,000*', Forbes, 3 September 2019). The CEO believed he was conversing with the CEO of the firm's German parent company, when in reality this was an elaborate facade. Synthetic identity software has spawned a new generation of identity fraud-related offences. As such, practitioners need to be aware of the nuanced threat that this technology creates.

This threat, however, is not isolated. With each new development, the potential for fraudulent use increases. The Internet of Things, for example, is but another invention that could be exploited. The Internet of Things is the term used to describe all devices connected to the internet, which can share and communicate data between each other. By pairing these devices with automated systems to glean information, the data retrieved can instruct the device to carry out a specific action. Here, the potential for wrongdoing is exponential. These vast stores of data could be a fraudster's paradise, waiting to be hacked, stolen and then used for illicit means. It may be possible to manipulate this data so that an automated and connected system can be fooled into carrying out financial transactions, which it would believe were being commanded by a legitimate user. What is more is that hacking one connected device might allow for the infiltration of the whole connected network. Compound this with the impending widespread introduction of 5G by the end of 2020, inter-device connectivity will be at its fastest level yet, perhaps making its users even more vulnerable to abuses.

Moreover, fraud has become almost synonymous with the concept of digital currencies and their associated technologies. Cryptocurrency security firm, CipherTrace, reported that in the first half of 2019, fraudsters stole over $4.26 billion in crypto-centric scams. The key problem here is that ordinary users are not equipped with the technical knowhow to allow for safe usage. Often fraudsters pray on this knowledge shortfall and exploit the information gaps in the system. While the same can be true of any fraud that targets lack of understanding, the scale of the problem and the rate at which crypto-frauds are spreading in popularity indicate that there is something to be said for the complexity of the technology.

The OneCoin scandal illustrates this. Billed as the cryptocurrency to rival Bitcoin, more colloquially known as the *'Bitcoin Killer'*, OneCoin duped investors worldwide out of $4.4 billion. It was unearthed that the usual promises of enhanced personal fiscal control and OneCoin's very own Blockchain, were entirely fabricated. Not only did the Blockchain never exist, but there was no mechanism in place to exchange OneCoin for any other form of currency, essentially prohibiting users from cashing out. As a result, OneCoin's founder Dr. Ruja Ignatova disappeared without a trace in 2017, when the company started taking heat. Undeterred, the US authorities have shifted the focus of the case to Dr. Ignatova's brother who has now pleaded guilty to several charges including money laundering and is facing up to 90 years in prison.

Here, asset tracing and recovery has been significantly hampered because of the added hinderance created by one of the key characteristics of cryptocurrency. Anonymity. All crypto-transactions are anonymised and therefore the ability of nefarious actors to use these anonymity provisions to evade legal ramifications is a significant problem. For instance, anonymity can be manipulated via the use of public keys, which are the cryptographic public addresses that Blockchain participants use to send virtual

currencies to one another. As the public key address is the only information available on the Blockchain, this presents a significant hurdle for enforcement agencies when tracing illegal activity. Following the Bitcoin (for example) will only ever lead to an account holder's public key. With no identifying information, and the fact that this could merely be one of many accounts held by the individual using false identities, prosecution and asset recovery becomes significantly more problematic.

Nevertheless, whilst it may seem that the March of Technology has in some cases outpaced the law, it can in other circumstances prove vital in the curtailment of frauds. The surge in use of technology assisted review has reduced the cost and hours spent on document review in cases that are often heavily burdened with information. More impressive still is the concept of *'Deeplearning'* technology. Deeplearning is technology that can be used to build up a picture of a person's usual financial transactions to then monitor specific account data. As a result, it can be used to pattern-spot and trace irregular financial transactions that do not conform to the usual sequence. These processes create a vital way to wade through vast amounts of data faster and more effectively than humans.

VII Recent developments and other impacting factors

Of the host of recent developments impacting fraud and asset recovery in England & Wales, none could be more prevalent than Brexit. On an immediate level, the immense confusion and uncertainty that has surrounded the (now exceedingly more imminent) departure from the European Union, may have created added difficulties that now need to be surmounted when it comes to tackling fraud. There is no completely definitive answer as to what legal or regulatory rules will remain in place if and when we leave. Nor is there absolute certainty as to what replacements or changes will come into force.

Fraud is rarely hampered by geographical borders and international cooperation is vital in order to have a modicum of hope in repatriating misappropriated funds that have been stashed overseas. Take for instance cyber-frauds. Funds can be bounced from proxy-server to proxy-server and across international borders in a matter of minutes. To date, this jurisdiction has tackled the problem by utilising international counter-fraud teams via the sharing of information and collaborating with cross-border enforcement bodies. Additionally, civil recovery orders, which are used to retrieve stolen funds, can easily be enforced in any European Union Member State *'without any special procedure being required'* under Chapter III, Article 36 of the Brussels 1 Regulation (Recast), as if it were a judgment rendered in that Member State. When we leave, the Brussels Regulations will cease to have effect. While we do not know what will replace this instrument, it is fair to say that there may be (at least in the transition from old instrument to new) a period where asset recovery is slightly more problematic. Brexit complicates the potential for free movement of information, or at the very least adds a curve to a relatively streamlined approach to enforcement.

It is not possible to speculate exactly what the future will hold. Although it is true that we will need to craft new instruments with different countries, we already have templates in place in the form of bilateral agreements with key players such as Cyprus, Germany and Italy. A new era for change is upon us and with this comes opportunity. As a jurisdiction, England & Wales has always been, and will remain, a vital player at the epicentre in the fight against economic crime. The Commercial Court 2019 Report in Subsection I, indicates just that. Moreover, we are investing in legal infrastructure projects to sure-up this reputation. For instance, the new purpose-built cybercrime, fraud and economic crime court, which is currently under construction in London and is due for completion in 2025, is but one example of the strides that have been made to keep the English courts ahead of the curve in the sector.

Another example is the revolutionary move made to curtail the increasing threat posed by cryptocurrency frauds. One of the fuelling factors that has led to the rise of this type of criminality, is the lack of standardised classification. Therefore, *The LawTech Delivery Panel Legal Statement on Cryptoassets and Smart Contracts*, published by the UK Jurisdiction Taskforce in 2019, suggests that the way to surmount this is to universally class these products as property. As per the statement, *'proprietary rights are recognised against the whole world'*. Therefore, by advocating for the attachment of property rights onto cryptoassets, if cryptoassets are misappropriated, we can now use the standing tools we have for the recovery of *'traditional'* properties in the crypto-sphere, across multiple borders. The Chancellor of the High Court, and Chair of the UK Jurisdiction Taskforce, Sir Geoffrey Vos, stated that this was *'a watershed for English law…Our statement…is something that no other jurisdiction has attempted'*. A world first, by formally

suggesting the blanket covering of cryptoassets as property, this demonstrates the innovative nature of the English courts in their attempt to create an organic and usable tool that applies existing mechanisms in nuanced settings. By attempting to enhance certainty amidst the confusion, the English courts are sending the message that they are a global leader in this domain. For a detailed discussion on the impact of crypto-criminality, please see Subsection VI.

The unimpeachable reputation of our court system, compounded by its ingenuity and creativity when it comes to assisting the victims of fraud seeking to be made whole again, is well-known. The wealth of intermediary orders that can be deployed, such as search and seizure orders, confiscation orders, passport orders and freezing orders both domestic and worldwide, will continue to be successfully utilised to offer meaningful remedial recourse. It is certain that while Brexit may cause a level of disruption in the immediate aftermath, depending on the exit strategy employed, the potential new freedom to create fresh legal tools may be a well-timed venture that can invigorate the current system used to fight fraud, as it battles with key impacting factors such as technological advancement and increased globalisation.

Keith Oliver specialises in commercial, regulatory and trust litigation. A renowned litigator and excellent practitioner, Keith is recognised as one of the world's best investigative lawyers and leads the firm's international strategy.

Keith has spent his career specialising in international disputes and the location, freezing and recovery of misappropriated assets involving emergency relief procedures and the management of legal teams from many jurisdictions. His work often involves multi-jurisdictional actions in the USA, continental Europe and worldwide. He is widely recognised as one of the UK's leading lawyers in civil fraud with a reputation for addressing and resolving the most intractable of disputes and crises faced by individuals and companies.

Keith is consistently ranked as a 'leading lawyer' in both *The Legal 500* and *Chambers and Partners* legal directories in the Commercial Litigation, Civil Fraud and Fraud categories.

keoliver@petersandpeters.com

Amalia Neenan is the civil and commercial legal researcher at Peters & Peters Solicitors LLP in London. Having been called to the Bar of England & Wales in 2015, Amalia then completed a Masters in International Business Law at the London School of Economics and Political Science in 2019, where she specialised in cryptocurrency frauds and the intersect between the law and technology. Amalia recently lectured on this topic in Cyprus as part of the McNeil International Symposium on Laws and their Applications for Sustainable Development. She regularly co-authors articles in this area with the head of international at Peters & Peters. Amalia is also a professional mentor for the nationwide charity The Girls' Network, which partners young women from underprivileged backgrounds with female professionals from a variety of different sectors and industries.

aneenan@petersandpeters.com

Hong Kong

Dorothy Siron
Zhong Lun Law Firm

With over 7.4 million people of various nationalities in a 1,104-square-kilometre (426 sq. mi.) territory, Hong Kong is one of the most densely populated places in the world. As a special administrative region, Hong Kong still maintains separate governing and economic systems from that of Mainland China under the principle of "one country, two systems". As one of the world's leading international financial centres, Hong Kong has a major capitalist service economy characterised by low taxation and free trade, and the Hong Kong dollar is the eighth most traded currency in the world. (The territory's 2,755 km^2 (1,064 sq. mi.) area consists of Hong Kong Island, the Kowloon Peninsula, the New Territories, Lantau Island, and over 200 other islands.)

Within this legal and economic framework, Hong Kong has become and still looks to be a hotbed for bank and cyber frauds and other financial, white-collar crime.

We look to discuss the legal framework that exists to assist a 'victim' of such white-collar crime to see what help is available to seek redress.

1 Key legal and statutory framework used in Hong Kong to pursue fraud, asset tracing and recovery cases

Hong Kong has a variety of legislation which provides for criminal offences relating to fraud.

The primary legislation for the main offences relating to fraud are the Crimes Ordinance (Cap. 200) (CO) and the Theft Ordinance (Cap. 210) (TO). These include:

i. fraud under section 16A of the TO;
ii. conspiracy to defraud under section 159E(2) of the CO;
iii. the basic definition of theft under sections 2 and 9 of the TO;
iv. offences involving deception, such as obtaining property or pecuniary advantage by deception under sections 17 and 18 of the TO;
v. offences relating to documents, such as forgery under section 71 and copying, using, using a copy of or possessing a false instrument under sections 72, 73, 74 and 75 of the CO;
vi. offences related to technology, such as altering or erasing data which constitutes destroying or damaging property under section 60 of the CO or accessing a computer with criminal or dishonest intent under section 161 of the CO; and
vii. any person who aids, abets, counsels or procures the commission by another person of any offence, is guilty of the underlying offence under section 89 of the Criminal Procedures Ordinance (Cap. 221).

Additional offences may also be found in

the Securities and Futures Ordinance (Cap. 571), Companies Ordinance (Cap. 622), Telecommunications Ordinance (Cap. 106) and Inland Revenue Ordinance (Cap. 112).

In Hong Kong, there are also various civil causes of actions which are available to a party who is a victim of fraud, such as:

Proprietary claim based on constructive trust

This allows a defrauded party to obtain relief in equity by claiming that the fraudster held the fraudulently obtained assets on constructive trust in favour of the defrauded party, and therefore the fraudster is held to account as a constructive trustee.

Third parties may also be liable if they are sufficiently implicated, in that they knowingly received fraudulently obtained assets.

Proprietary claim based on unjust enrichment (money had and received)

This allows a defrauded party to claim that the fraudster was enriched at the expense of the defrauded party in circumstances which are unjust, such as where there is a total failure of consideration or a mistake of fact or law.

Tort of conspiracy

Where a defrauded party's interests were injured by use of unlawful means (i.e. fraud) by two or more persons who conspired together to do so, the defrauded party may bring a tortious claim of conspiracy against the fraudsters.

The defrauded party does not need to show there was actual damage or that damage was the main purpose, just that the intention of the conspiracy was to cause damage to the defrauded party.

Fraudulent misrepresentation

Where a fraudster has made a representation knowing it to be false or without actual belief in the truth of the representation (i.e. recklessly) and a defrauded party relies on the representation and suffers loss as a result, a defrauded party may bring a tortious claim of deceit based on fraudulent misrepresentation.

As a spring board for the civil claims that a victim can launch, there are a variety of orders which may be sought in the interim that allow for the freezing of assets, such as bank accounts, and tracing and discovery of assets which victims can look towards.

Norwich Pharmacal order

An order against a third party for disclosure of documents and information which allows the defrauded party to trace the passage of information or assets prior to starting proceedings against the fraudsters. The disclosure is generally restricted to information which allows the defrauded party to identify and go after the fraudsters.

This principle was established in the English case *Norwich Pharmacal Co v Customs & Excise Commissioners* [1974] AC 133 and has been applied in Hong Kong repeatedly.

A banker's trust order

A form of relief derived from the English Court of Appeal's decision in *Bankers Trust Company v Shapira* [1980] 1 WLR 1274 which is essentially an NPO directed at third-party banks or professional advisers. This order directs them to provide information which enables tracing of assets but which normally is protected by confidentiality.

Disclosure has been extended by the Hong Kong Courts to discovery of bank books and other documents including bank statements and account opening forms.

Bankers' records/books order

Any party to any legal proceedings may apply to the Court, under section 21 of the Evidence Ordinance (Cap. 8) ("**EO**"), for an order that a bank allow that party to inspect and take copies of its records/books for the purposes of discovery.

The disclosure is generally limited to documents necessary for the purpose of those particular proceedings.

Mareva injunction

This is a freezing order which a defrauded party may apply to the Court for in order to prevent a fraudster from dealing with, moving or disposing of assets. Courts in Hong Kong apply the principles set out in the English case *Mareva Compania Naviera SA v International Bulk Carriers SA [1980] 1 All ER 213*.

A freezing order can apply to all asset classes including, but not limited to, property, bank accounts, shares, account receivables and chattels.

Such an order can restrain fraudsters from dealing with their Hong Kong assets only (domestic *Mareva*) or can prevent fraudsters from dealing with assets outside Hong Kong as well (worldwide *Mareva*).

An order is also binding on third parties who are served with the order; therefore, it is common to serve such orders on banks at which the fraudsters have accounts in order to get those accounts frozen.

Hong Kong Courts may also enforce worldwide *Mareva* injunctions obtained overseas in Hong Kong by getting a local domesticated equivalent injunction order under section 21M of the High Court Ordinance (Cap 4) (HCO).

Anton Piller order

This is a search and seizure order to assist with the preservation of documents. This order will allow the defrauded applicant to enter the premises of the fraudster – search for and remove documents relevant to the applicant's case.

Prohibition against debtors from leaving Hong Kong

A defrauded party which has a judgment in its favour – therefore a judgment creditor – may apply to the court for an order to prevent a debtor fraudster from leaving Hong Kong to another jurisdiction. Armed with a prohibition order which has been served on the Immigration Department, the fraudster would be stopped from departing Hong Kong at check points pursuant to Order 44A of the Rules of the High Court (Cap. 4A).

The Prohibition Order is usually valid for one month, and renewable for two further one-month extensions.

Interim attachment of property

Where a defendant fraudster in an action is about to dispose of property or (any part thereof) with the intent of obstructing or delaying the execution of any judgment, a defrauded party may apply to court for an order that the fraudster furnish security which would be enough to satisfy any judgment that may be given against the fraudster pursuant to Order 44A of the Rules of the High Court (Cap. 4A).

With all of the cases coursing through the Hong Kong Courts, there is no lack of cases illustrating the effectiveness of Hong Kong's system.

CXC Global Japan Kabushiki Kaisha v Kadima International Ltd [2019] HKEC 3988: this is a typical email fraud case which illustrates the main stages of fraud, asset tracing and recovery.

The defrauded plaintiff is a Japanese company and the two defendants are Hong Kong companies which maintained bank accounts with OCBC Wing Hang Bank Limited (OCBC). The plaintiff was duped into transferring US$108,632.50 into the defendants' bank accounts in the belief that the instructions were for a merger and acquisition planned by the chairman of the group of companies the plaintiff belonged to – this is an illustration of your typical CEO fraud.

The plaintiff obtained proprietary and *Mareva* injunctions, as well as bankers' books orders, against both defendants. Pursuant to the bankers' books orders, the plaintiff obtained account statements and transaction records of both defendants' accounts.

The plaintiff filed a writ of summons and then sought, by way of summons, a default judgment against the defendant, as well as to join OCBC to seek a vesting order for the sum of US$108,632.50.

The second defendant was absent from the summons hearing. Default judgment was obtained against the first defendant and the court found that the sum of US$90,000 in the second defendant's OCBC account was held on constructive trust for the plaintiff, thus OCBC was ordered to pay that sum to the plaintiff.

The effectiveness of the Hong Kong system can particularly be seen with regards to how it handles new challenges, such as the general increase in online business fraud, email fraud and investment fraud cases in recent years.

Hong Kong courts have shown an increased willingness to assist victims of such frauds, notably by granting declaratory relief to victims at an interlocutory stage of proceedings, without trial.

Recently, in *Skandinaviska Enskilda Banken SA v Hongkong Liling Trading Ltd* [2018] HKCFI 2676, a victim of email fraud claimed that the funds the defendant had defrauded from it were held on trust for the victim by way of a proprietary constructive trust.

The court granted default judgment along with a declaration that the defendants held the funds on trust for the plaintiff.

While the Court noted that "a court will not normally make a declaration without a trial", it viewed there was a genuine need for declaratory relief in which "the practice will give way to the requirements of justice".

The same reasoning has been followed in a number of other recent first-instance judgments in the High Court and the District Court.

In another recent case, *Terence John Stott v Larks Trading Ltd* [2019] HKCFI 1317, the victim of a fraudulent investment scam brought a claim based on proprietary constructive or resulting trust and seeking default judgment. The Court again granted the victim declaratory relief without a trial.

Does the regime go far enough in the pursuit of fraudsters and the recovery of stolen assets?

In other jurisdictions, courts and regulators have sought to share the burden with the banks opening these accounts, but in Hong Kong, it seems that one can still open a bank account with a shelf company with relative ease and facility. Hence fraudsters are still able to open bank accounts which act as recipient accounts for proceeds of fraud. Notwithstanding the foregoing, the banks in Hong Kong still require very stringent risk assessment of the information they collect and the individuals whom they allow to open bank accounts, to fulfil their AML requirements,

whether under individuals' names or corporate accounts; otherwise, Hong Kong will continue to remain an attractive jurisdiction for would-be money launderers.

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

Main stages of how fraud, asset tracing and recovery cases are approached in Hong Kong

Early steps: contacting law enforcement, banks involved and engaging lawyers

Contacting law enforcement: defrauded parties may look to the Hong Kong Police Force and other authorities such as the Joint Financial Intelligence Unit (JFIU) (which is jointly run by officers from the Hong Kong Police Force and the Hong Kong Customs & Excise Department), the Commercial Crime Bureau, the Organized Crime and Triad Bureau or the Independent Commission Against Corruption. An online police report should be filed to register the fraud at the earliest opportunity.

The police may require the bank receiving fraudulently obtained assets to temporarily block any attempts to transfer or withdraw the assets.

At all times, the victim should first try to contact both the company's own outward remitting bank and the recipient bank to obtain information about the status of the transfer and the whereabouts of the funds being remitted.

Lawyers can also be retained to issue letters to the recipient banks to point out any potential criminal consequences of transferring or dealing with the funds which they know or suspect to be the proceeds of crime (*section 25 of the Organised and Serious Crimes Ordinance*).

A letter to a bank which sets out details of the fraud and points out the potential criminal consequences of moving the funds may make a bank pause before honouring transfer instructions received from a fraudster, and buy time to freeze the money by other methods.

The police in both the jurisdiction of the outgoing funds and the jurisdiction to which the money has been transferred should also be alerted.

Commencing civil proceedings, which may be done together with tracing and identifying assets and freezing or restraining assets (explained further below):

Once the defrauded party's money has arrived at a local bank account, there is no means by which the recipient bank would voluntarily reverse the transaction. Hence the defrauded party should commence private civil proceedings in the Hong Kong courts against parties holding or having an interest in the assets/property sought to be recovered, namely the bank account holder in the case of a bank account fraud.

The most common relief sought for fraud is damages, although other remedies such as equitable relief (e.g. a proprietary claim based on constructive trust) may also be sought.

Tracing and identifying assets

The defrauded party should make sure that there are identifiable assets/property in Hong Kong which may be restrained or confiscated, as authorities in Hong Kong cannot act on any request to restrain or confiscate assets which does not identify particular assets/property.

The relationship between the identified assets/property and the defendants should also be shown

and established. If the assets/property are held by third parties, then one must establish the basis upon which confiscation is sought.

The defrauded party may also need more information or evidence about the assets/property of the fraudster. Aside from searching public resources, such as the Land Registry or the Companies Registry, and the statutory rules in Hong Kong on the discovery and inspection of documents for parties to civil proceedings, the defrauded party has the option of making applications for discovery orders such as *Norwich Pharmacal* orders, banker's trust orders or bankers' records/books order under section 21 of the EO.

These are important for acquiring information or evidence about fraudsters, or the fraudster's assets from third parties.

Freezing or restraining assets under a court application for an injunction

There are various forms of interim relief available to restrain fraudsters from dealing with, moving or disposing of assets, such as obtaining a *Mareva* injunction or an *Anton Piller* order as discussed above.

A hearing for such interim relief may be obtained at short notice and is heard *ex parte*, and the court will issue the freezing order if it is satisfied that the required conditions for making the order are met. The initial order to freeze assets is an interim order for a limited period only and parties will be given time to effect service of the order and related documents on the defendant fraudster(s) and other affected parties, such as banks.

Parties will then get a return date to go back to court, at which point they will need to provide to the court evidence that service on the defendant fraudster(s) and other affected parties was effected. The defendant fraudster(s) and other affected parties may appear at this hearing.

If the defendant fraudsters and other affected parties do not appear, normally the court will grant a continuation of the freezing order "until further order of the court" so it will remain effective until the proceedings are complete.

Recovering assets and enforcing judgments

Once assets have been frozen in Hong Kong, the proceedings will need to continue to be litigated, as frozen assets cannot be recovered until the defrauded plaintiff has obtained a final judgment and executed on the judgment.

In cases where the defendant fraudster(s) does not participate in the civil proceedings and fails to file an acknowledgment of service of a defence – as is common in email fraud cases – the defrauded plaintiff can obtain a default judgment (judgment without a trial) against the defendant fraudster(s).

Obtaining a summary judgment – where the defendant has no defence to the claim – is generally not available to plaintiffs where their claim is based on an allegation of fraud as the court has no jurisdiction to grant summary judgment in such cases.

However, in recent years there have been some cases where the fraud exception did *not* automatically apply where the facts of the case include fraud, but the defrauded plaintiff could show the claim would succeed even without proof of fraud.

For instance, in *Laerdal Medical Limited v Hong Kong Haocheng International Trade Limited* HCA 2193/2016, the plaintiff showed its case could succeed based on unjust enrichment without proving fraud. The court also additionally found, for various reasons, that the defendant's "defence is hopeless".

Types of relief after successfully obtaining a judgment include:

1. *Mareva* injunctions in aid of enforcement;
2. the appointment of a receiver;
3. examining the judgment debtor(s) (who were the fraudster defendants), if available, on oath in order to identify the whereabouts of the assets of the judgment debtors; or
4. discovery or disclosure of documents against third parties.

There are a variety of methods for enforcing such judgments, such as garnishee proceedings and charging orders.

Garnishee proceedings are against a third party, typically the local bank with which the defendant fraudster has an account containing

the fraudulently obtained assets. A garnishee order attaches the debt claimed to be due and accruing from the garnishee to the judgment debtor, i.e. money in the judgment debtor's bank account, and will require the bank to pay the money directly to the defrauded plaintiff as part of the execution of a judgment obtained by the defrauded plaintiff.

Where the defendant fraudster has assets, such as landed property, securities or funds in court, the defrauded plaintiff can try to obtain a charging order to impose a charge over those assets. This provides the defrauded plaintiff with security, though further action would have to be taken to realise those assets.

Other options, depending on the circumstances, include writs of *fieri facias*, writs of sequestration, winding-up proceedings or bankruptcy proceedings and orders for committal.

What are the benefits to this system and are there any difficulties?

Generally speaking, the Hong Kong legal system and its courts are well-equipped to deal with disputes and cases which result from fraud and also provide relief to those parties who have fallen victim.

However, the process discussed above does take time, and if the various orders discussed above are not obtained quickly enough, particularly to freeze misappropriated assets in the fraudster's bank accounts, it is likely the fraudster will have already transferred those assets elsewhere (usually out of the jurisdiction) (discussed further in section 4 below).

3 Parallel proceedings (a combined civil and criminal approach)

There are no restrictions on civil proceedings progressing in parallel with criminal proceedings on the same subject matter. A combined civil and criminal approach occurs frequently in Hong Kong; however, not at the request of the victim but rather at the discretion of the Police. Once a party has been defrauded, there is much advantage to be gained from reporting the fraud online as described above. With that report, it is hoped that the Police will get involved to impose and issue a 'letter of no consent' to the bank, informing the bank that the Police do not consent to their handling or dealing with the fraudster's account. The JFIU would determine whether such a letter should be issued. Having said that, however, this is not something that the victim of a fraud can 'order' or insist that the Police do, and if the Police do issue such a letter then the victim can save on legal fees as the bank account will be frozen without a court order.

The Police may have powers to freeze a bank account much more quickly by issuing a 'letter of no consent', and it is possible that the police may assist in recovering stolen funds or even carry out the recovery process themselves.

The 'letter of no consent' procedure in Hong Kong:

i. When fraud is reported to the JFIU, including as a suspicious transaction report (STR), the JFIU issues a "letter of no consent" to a bank. This means that JFIU does not consent to the bank dealing with the funds in the account.
ii. Section 25A of the Organized and Serious Crimes Ordinance (Cap. 455) (OSCO) requires a person (an "informant") to disclose his/her knowledge or suspicion that any property represents the proceeds of crime to the JFIU. If the JFIU gives the informant consent to deal with the property, the informant does not commit an offence under section 25 if they deal with the property.
iii. If the JFIU does not give consent to the bank to deal with the property (the "no consent" regime), the informant or bank cannot deal with the property because this will constitute a criminal violation of section 25.
iv. However, section 25A(2)(a) and the "no consent" regime does not operate to withhold or freeze the accounts or property of a suspect. It only creates a defence for further dealings with the property after disclosure.
v. It remains for financial institutions to decide whether to honour the instructions of their

customers despite their suspicion and the disclosure.

vi. If, on the other hand, the Police do not issue the 'letter of no consent', the victim of the fraud is left with having to run into court to apply for typically a *Mareva* injunction to prevent further dissipation and a banker's records order to trace the funds, thereby having to incur legal fees.

Note on criminal proceedings in Hong Kong: For serious offences – which likely includes matters relating to fraud – there is no formal time limit for the commencement of a prosecution; in contrast to minor 'summary offences', which generally have a six-month limitation period starting from the commission of the offence (section 26 of the Magistrates Ordinance (Cap. 227)).

Benefits of the combined civil and criminal approach

Apart from civil causes of action and court orders that may be granted in civil proceedings, with respect to criminal matters, law enforcement agencies have certain powers to gather evidence and identify, trace, and freeze proceeds, while certain other actions to restrain and seize assets lie with the prosecutor.

The Hong Kong Police Force acts pursuant to the Police Force Ordinance with respect to evidence-gathering procedures and seizure of suspected property. Prosecutors will likely have the benefit of receiving evidence gathered by law enforcement. In particular circumstances, they may pursue their own applications to the court for evidence-gathering orders. The Police, however, do not share results of their investigations with the public and hence victims of fraud cannot rely on this as a resource for their civil claims.

Under section 15 of OCSO, a prosecutor may move for the restraint of assets or property to prohibit a defendant that has benefited from an offence specified under the ordinance – including those arising from fraud – from dealing with any realisable property. Where such a restraint order is in place, the court may appoint a receiver to take possession of any realisable property or otherwise manage or deal with such property. In addition, an authorised officer may also seize restrained property to prevent its removal from Hong Kong.

Section 16 of OSCO allows for the prosecutor to apply to the court for a charging order on realisable property, which has the effect of securing payment to the Hong Kong government backed by the property charged.

In any event, a discontinued or failed criminal prosecution is not a bar to civil action in Hong Kong since the standard of proof in civil proceedings is lower than in criminal proceedings.

The difficulties as mentioned above are that a victim of a fraud cannot expect to work in tandem with the Police, or rely on Police investigations to assist in the recovery of the funds, but rather must spend legal fees in its effort to recover the funds. The chicken or egg situation prevails because, at all times, victims would want to have certainty of recovery before deciding to spend good money after bad. To this extent, the legal practitioner is not in a position to advise with any certainty of outcome.

Civil fraud claims must be brought within six years from the date on which the cause of action accrues. This period does not begin until the defrauded plaintiff discovers the fraud or could, with reasonable diligence, have discovered it.

Plaintiffs, however, cannot act against an innocent third party who purchased the property for valuable consideration and without notice of the fraud, i.e. the defence of *bona fide purchaser for value without notice* prevails. In other words, at the time of the purchase, where the third party did not know or have reason to believe that a fraud had taken place.

4 Key challenges

Banks have contractual duties to their customers, which usually include the duty to honour any instructions to transfer funds out of a bank account before any injunction order is granted by the court and/or any action is taken by the authorities.

Given also that it can take time to communicate the details of a fraud to the right person in a large banking organisation and to persuade them to take action, it may be that a recipient bank can do, or will do, nothing to stop further transfers of the monies.

It can take time to communicate the details of a fraud to the right individual in a large banking organisation and to persuade them to take action, so it may be that a recipient bank can do, or will do, nothing to stop further transfers of the monies promptly.

The defrauded monies may have been transferred out of the bank account of the fraudster defendant.

The defrauded monies may also have been transferred out of jurisdiction; if the defrauded monies have been transferred to the People's Republic of China, it would be particularly difficult to recover the same.

Furthermore, commencing civil proceedings and taking out the interlocutory applications mentioned earlier in this chapter can come with a significant legal cost and there is no guarantee that the defrauded party will recover all, or even any, of their money.

5 Cross-jurisdictional mechanisms – issues and solutions in recent times

Most frauds now span multiple jurisdictions and often the cross-border litigators may need to cooperate and be involved or mobilised with despatch quickly to try and arrest the funds.

Given that Hong Kong is an international hub where the incorporation of private limited companies is inexpensive and relatively easy and banks are accustomed to customers dealing in large amounts of money, Hong Kong is a popular destination for fraudulently obtained funds to be transferred to, particularly in email fraud cases.

In August 2015, the United States' Federal Bureau of Investigation (FBI) reported that the majority of wire transfers in fraud cases involving business email compromises were going to Asian banks located within Hong Kong and China.

In July 2018, the FBI reported again that Asian banks located in Hong Kong and China remained the primary destinations of fraudulent funds where wire transfers were made pursuant to business email compromises/email account compromises.

The mechanisms in place for effective tracing of assets cross-jurisdictionally

Criminal proceedings

Article 96 of the Basic Law provides that with the assistance or authorisation of the Central People's Government, the Hong Kong Government may make appropriate arrangements with foreign states for reciprocal juridical assistance.

There are also several multilateral agreements which apply to Hong Kong which provide for mutual legal assistance in criminal matters. Hong Kong also has bilateral mutual legal assistance agreements with 30 other jurisdictions as of November 2018.

As a matter of common law, the Hong Kong Police can exchange information with and release information to law enforcement bodies in other jurisdictions (such as the FBI) for intelligence and investigation generally.

The Hong Kong Police also has mutual assistance arrangements with enforcement bodies of other countries where assistance is required across jurisdictions for situations such as the obtaining of information for use in a prosecution or the production of materials relating to a criminal matter from the party in possession or control of those materials Such a request will be dealt with under Hong Kong's mutual legal assistance framework and be processed under the Mutual Legal Assistance in Criminal Matters Ordinance (Cap. 525) (MLAO).

The MLAO was enacted so that Hong Kong's law enforcement authorities could work with their counterparts abroad in investigating and prosecuting criminal offences. It provides for a variety of legal assistance available which is important in the context of asset tracing.

Under the MLAO, the Secretary of Justice of Hong Kong may provide assistance to another jurisdiction or make requests to another jurisdiction for assistance of the types set out in the MLAO. These include:

1. taking and production of evidence;
2. search and seizure;
3. production of material;
4. transfer of persons to give assistance in relation to criminal matters;
5. confiscation of proceeds of crime; and
6. service or certification of documents.

These types of assistance allow Hong Kong to work with other jurisdictions to get orders to trace assets, such as by getting a bank to produce documents, as well as to freeze or confiscate assets.

Where the jurisdiction making a request to Hong Kong does not have a bilateral agreement with Hong Kong, that jurisdiction will need to provide a reciprocity undertaking. Otherwise, Hong Kong will refuse such a request.

However, section 3 of the MLAO specifically provides that it does not apply to the provision or obtaining of assistance in criminal matters between Hong Kong and any other part of the People's Republic of China.

Parts VIII and VIIIA of the Evidence Ordinance (Cap. 8) (EO) also provide that the court of first instance in Hong Kong has the power to assist in obtaining evidence for criminal proceedings in an overseas court, as well as the power to order that a letter of request – a formal written request – be issued to an overseas court to assist in obtaining evidence for criminal proceedings in Hong Kong.

Civil proceedings

Part VIII of the EO provides that the Hong Kong courts have the power to assist in obtaining evidence for civil proceedings in overseas courts.

Order 70 of the Rules of the High Court (Cap. 4A) (RHC) then provides the framework for the Hong Kong courts to obtain evidence for overseas courts pursuant to Part VIII of the EO or pursuant to The Hague Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters (the Hague Evidence Convention), which Hong Kong is a contracting party to. The Hague Evidence Convention provides a mechanism for the 61 states which are contracting parties to obtain evidence located overseas by issuing a letter of request.

Letters of request (also known as letters rogatory):

A foreign defrauded party may get the judicial body of the overseas jurisdiction in which they commenced proceedings to issue a 'letter of request' to Hong Kong courts for assistance in obtaining evidence in civil proceedings. The jurisdiction of Hong Kong courts to do so is provided under Part VIII of the EO.

A Hong Kong court may also issue a letter of request to foreign courts to acquire evidence from parties out of the jurisdiction based on the Hague Evidence Convention.

Where a letter of request is from a foreign country which is not a party to the Hague Convention, it can still be recognised even though no convention is in force. The language of Part VIII of the EO is wide enough to provide for requests from states which are not parties to the Hague Evidence Convention (*Order 70, Rules of the High Court*).

While China is also a contracting party to The Hague Evidence Convention, it does not apply between Hong Kong and China since they are two jurisdictions within the same state.

Hong Kong and China separately entered into the Arrangement on Mutual Taking of Evidence in Civil and Commercial Matters between the Courts of the Mainland and the Hong Kong Special Administrative Region, which came into force on 1 March 2017.

This arrangement assists parties to proceedings in Hong Kong and China in obtaining evidence in civil and commercial matters with greater efficiency and certainty.

Foreign defrauded parties may also freeze and realise proceeds of fraud in Hong Kong by way of Section 21M of the High Court Ordinance (Cap. 4) (HCO):

Under Section 21M of the HCO, the Hong Kong court has the jurisdiction to grant interim relief in relation to proceedings which have been or are to be commenced in a place outside of Hong Kong and are capable of giving rise to a judgment which may be enforced in Hong Kong.

This may provide a way for overseas victims of fraud which have identified assets belonging to the fraudster in Hong Kong to obtain interim relief, such as a *Mareva* injunction, in respect of those assets. The overseas victim may then continue pursuing their proceedings overseas without having to conduct concurrent proceedings in Hong Kong.

6 Technological advancements and their influence on fraud, asset tracing and recovery

While the integration and use of artificial intelligence (AI) in the legal sector in Hong Kong is in its early days, law firms in Hong Kong are increasingly welcoming and embracing the use of technology in providing legal services.

This is likely to be the trend for most, if not all, law firms in Hong Kong in the next few years. So far, the legal sector has largely integrated and utilised technology, including AI and machine learning, in areas such as e-discovery, due diligence, contract review and repetitive document management exercises, as those are areas where the volume of data and/or documents can be so massive that human review is either almost impossible or exceedingly difficult or not cost-effective. Use of technology to assist makes it faster, more accurate and more cost-effective to carry out such tasks.

Hong Kong has also seen various start-ups take integration of technology into the legal sector beyond just large-scale document review and management, such as:

i. the Hong Kong-based Zegal, which offers cloud legal software solutions for both law firms and businesses by simplifying the search for legal documents and automating the legal document drafting process; and
ii. the not-for-profit Electronic Business Related Arbitration and Mediation, also known as "eBRAM", which is developing a new online platform for dispute resolution in which users can go through negotiation, mediation and arbitration entirely online and AI will facilitate deal-making on this platform. This was formed with the support of the Law Society of Hong Kong and the Hong Kong Bar Association.

However, there are not yet any specific examples of technology being used by Hong Kong's legal sector to aid fraud, asset tracing and recovery in Hong Kong, save for individual service providers' own search engines.

The advancement of technology vs the difficulties of asset traceability?

An example of a situation in Hong Kong where tracing assets was made more difficult due to the advancement of technology is the launch of the Faster Payment System (FPS) in September 2018 in Hong Kong.

FPS is a real-time payment system introduced by the Hong Kong Monetary Authority and operated by Hong Kong Interbank Clearing Limited to allow for immediate fund transfers and retail payments between consumers and merchants. All banks and e-wallet operators in Hong Kong can participate in the FPS.

However, soon after the launch of the FPS, fraud cases involving the FPS cropped up as a result of fraudsters stealing personal and bank account information of victims, then using this information to open up fake e-wallets and then stealing money from those victims' bank accounts using the fake e-wallets.

Real-time transactions leave more room for fraud because unlike traditional payment methods which take more time to go through, making payments through systems like the FPS are immediate and irreversible. Therefore, once your money is gone, it is essentially gone for good.

As for cryptocurrencies and virtual assets generally, with the rapid development of virtual assets, frauds related to virtual assets have also risen.

Hong Kong turned into a flourishing market for cryptocurrency exchanges and initial coin offerings (ICOs), given that its rules on virtual currencies are less strict than those in China, where ICOs and cryptocurrency exchanges have

been banned since 2017 (and now essentially all crypto-related commercial activities are banned).

By February 2018, however, the Securities and Futures Commission of Hong Kong (SFC), the statutory authority in Hong Kong which regulates the securities and futures markets, announced that they had received several complaints from cryptocurrency investors against issuers of ICOs alleging "unlicensed or fraudulent activities" or that cryptocurrency exchanges had "misappropriated their assets or manipulated the market". The SFC also received complaints from investors who claimed they were unable to withdraw fiat currencies or cryptocurrencies from accounts they opened with cryptocurrency exchanges.

In a number of other circulars, the SFC urged investors to be careful of the heightened risk of – among other problems – fraud when investing in cryptocurrencies and ICOs.

Given that such investments, along with the use of cryptocurrency exchanges, occur online, a victim of fraud may have trouble pursuing fraudsters if those fraudsters are not physically present in Hong Kong.

SFC also flagged that it may not have jurisdiction over issuers of ICOs or cryptocurrency exchanges if "they have no nexus with Hong Kong or do not provide trading services for cryptocurrencies which are 'securities' or 'futures contracts'".

Further, since digital tokens involved in ICOs are transacted or held on an anonymous basis, they pose inherent risks

The SFC also noted that these technological advancements were causing an increase of intermediaries who were starting to provide asset management services involving virtual assets.

The SFC publicly expressed concern about virtual asset portfolio managers and virtual asset trading platform operators in November 2018, as these portfolio managers and platform operators may not carry out enough due diligence before they invest in a certain virtual assets or allow a virtual asset to be traded on their platforms. Therefore, investors may end up being defrauded and lose their investments.

How has the law kept up with these advancements or is it lagging behind?

Since Hong Kong is still in its early days of seeing the impact of technological advancements on issues such as fraud and also utilising technological advancements in the legal sector, there has not yet been much visible influence on the law.

However, statutory bodies such as the SFC have worked to address issues which have come up so far, such as to try to bring virtual asset portfolio managements into the SFC's "regulatory net"

For instance, on 1 November 2018, the SFC announced a "conceptual framework for the possible regulation of virtual asset trading platforms" and subsequently met with virtual asset trading platform operators in Hong Kong to explain the SFC's regulatory expectations.

The SFC decided that it would be appropriate to regulate certain types of centralised platforms trading security and non-security virtual assets and published a framework for doing so in a Position Paper published on 6 November 2019. Where virtual asset trading platforms are able to meet the SFC's regulatory standards (which are similar to those for licensed securities brokers), the SFC will grant a licence to those platforms and regulate them under the SFC's existing powers.

However, the SFC pointed out in this paper that the SFC does not have the power to grant licences to or oversee trading platforms which only trade non-security virtual assets.

Furthermore, the parts of the Securities and Futures Ordinance (Cap. 571) which enable the SFC to take action against market misconduct in the securities and futures markets will not apply to licensed virtual asset trading platforms because, at the end of the day, they are still not a recognised stock or futures market and the virtual assets are not "securities" or "futures contracts" listed or traded on such a market (*paragraphs 1 to 9, SFC Position Paper on Regulation of virtual asset trading platforms*).

In 2018, the SFC also ordered a Hong Kong-based ICO issuer Black Cell Technology Limited (Black Cell) to halt raising capital through an ICO and return all digital tokens to investors, as Black Cell's activities may qualify as a "collective investment scheme" that would require the SFC's approval to market or sell to the general public.

7 Recent developments

There has been an increase in the use of "mule" bank accounts in Hong Kong for moving money obtained by way of fraud.

These mule bank accounts have other trading purposes and became an issue where the beneficiary of the subject bank accounts argued that they received the funds of the defrauded party as a '*bona fide* purchaser' and should be entitled to keep those funds.

Hong Kong saw a spate of these cases, such as *Laerdal Medical Limited v Hong Kong Haocheng International Trade Limited* HCA 2193/2016 (mentioned above), where the defendant claimed it had received funds from the defrauded plaintiff as consideration for a business transaction, which was a shipment of ladies' shoes from a company in Mainland China. However, the Hong Kong

court found that the defendant had a hopeless defence considering, among other factors, that the defendant had no contract with the defrauded plaintiff but the defendant's own banking documents showed the funds were credited in favour of the defendant by the plaintiff.

Similarly, in *Ferrari North America, Inc v Changhon International Energy Co. Limited and Others* HCA 862/2017, an email fraud case where the plaintiff was lured into paying US$6.7 million into the defendant's Hong Kong bank account. Part of this sum was transferred onward to other defendants and one of these defendants claimed it had received part of the funds as part of its "*bona fide* arm's length dealings" to buy frozen meat products from suppliers. In this case, the Hong Kong court found enough issues with the defendant's evidence to raise a suspicion of dishonesty – such as the defendant's sales confirmation being inconsistent with its other sales confirmations and the defendant's bank documents showing that it had no normal commercial banking or business-related activities at the time of the fraudulent transfers – and accordingly continued the injunction which the plaintiff had applied for to freeze the funds.

8 Conclusion

The landscape is ever evolving for this particular area of the law, and law enforcers and the courts can hardly keep up with some of the new and crafty ways fraudsters operate. Experience, exposure and public knowledge are certainly assets as most fraudsters will have a tried and true *modus operandi* whilst many victims are still not wary or vigilant enough to alert themselves to suspicious circumstances and are too quick to make assumptions of good faith and regularity.

Reform may be needed in banking governance and account opening vigilance so that fraudsters do not have the benefit of hiding behind the veil of privacy and restitutionary steps may be taken once any fraud is detected.

Cross-border sharing of information and skills will also help in fast-tracking any relief for the defrauded victims.

Dorothy Siron is one of the partners of Zhong Lun and heads up the Litigation and Dispute Resolution practice in the Hong Kong office.

Dorothy's practice focuses on complex cross-border commercial litigation and arbitration and international trade. She has expertise in several specialised areas of law, including commercial fraud, white-collar crime, cyber fraud, professional negligence, international trade disputes and enforcement of foreign judgments, contentious trust, probate and estate disputes, cross-border litigation, and family law work. Moreover, she frequently handles Mareva and other types of injunctions; enforcement; disciplinary actions against listed companies and its directors and officers by the Securities and Futures Commission; and enquiries by the Independent Commission Against Corruption (ICAC).

Dorothy is a Director of TerraLex, an international network of independent law firms, a past Committee Member of the International Committee of the National Asian Pacific American Bar Association (NAPABA) and an associate member of the Chartered Institute of Arbitrators, UK. She is also a member of the prestigious International Academy of Financial Crime Litigators and the International Association of Defense Counsel (IADC), membership of which are both by invitation only.

dorothysiron@zhonglun.com

Ireland

Karyn Harty
McCann FitzGerald

Audrey Byrne
McCann FitzGerald

Ireland has a sophisticated and respected courts system which is experienced in dealing with complex cross-border disputes. As a member state of the EU, Ireland benefits from the co-ordinated civil litigation procedures available under the Brussels I Recast Regulation (1215/2012) and other EU law regimes, and the large number of global companies locating their EU operations here often places Irish entities at the centre of global investigations.

The Commercial Division of the High Court has dealt with many cross-border claims and applications in aid of fraud litigation in other jurisdictions. This chapter provides an overview of the system, remedies available and the approach of the Irish courts to fraud and asset recovery litigation.

1 Legal framework and statutory underpinnings

Ireland, as distinct from Northern Ireland, a separate legal jurisdiction comprising six counties which form part of the United Kingdom of Great Britain and Northern Ireland (the UK), has a common law legal system with a written constitution and a Commercial Court experienced in dealing with complex litigation. Understanding the legal parameters for dealing with investigations into suspected fraudulent conduct is essential.

Criminal Justice (Corruption Offences) Act 2018

Ireland's anti-corruption laws were recently overhauled through the Criminal Justice (Corruption Offences) Act 2018. This legislation consolidated existing law and introduced a number of new criminal offences, closely informed by the UK's Bribery Act 2010, including active and passive corruption and corruption in relation to office, employment, position or business.

The Act also provides for a new corporate liability offence which allows a corporate body to be held liable for the corrupt actions of *inter alia* any of its directors, managers, secretary, employees, agents or subsidiaries, with the intention of obtaining or retaining business, or an advantage in the conduct of business, for the body corporate.

Some provisions have explicit extra-territorial effect, so that Irish persons, companies and other organisations registered in Ireland which commit acts outside Irish territory which would constitute an offence if committed within Irish territory may be prosecuted.

Regard should also be had to false accounting (Section 10 of the Criminal Justice (Theft & Fraud Offences) Act 2001) and offences relating to the falsification of company books and documents under the Companies Act 2014.

Anti-money laundering

As a member of the EU, Ireland is subject to EU legislation on the internal market, including the anti-money laundering and counter-terrorist financing framework. The Fifth Anti-Money Laundering Directive (MLD5) (EU) 2018/843 also applies (note: most of the Directive's provisions were to be transposed into national law by 10 January 2020; however, as of the date of publication, Ireland has not enacted the required implementing legislation).

Hacking and cybercrime offences

Cybercrime is an increasing concern for businesses and the Criminal Justice (Offences Relating to Information Systems) Act 2017 was specifically targeted at hacking and cybercrime. The Act created new cybercrime offences and transposes the requirements of the EU Cybercrime Directive (Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems). It also addresses the cross-border impact of cybercrime by contributing to a harmonious approach to the issue across the EU.

Mutual legal assistance (MLA)

Applications for mutual legal assistance (MLA) are also commonly brought in Ireland again because of the large number of online/digital content providers domiciled here.

Criminal Assets Bureau (CAB)

The Criminal Assets Bureau (CAB) brings together law enforcement officers, tax and social welfare officials as well as other specialist officers from different organisations. The CAB is an independent body corporate rather than part of the Irish police (*An Garda Síochána*) and has power to take all necessary actions in relation to seizing and securing assets derived from criminal activity. It is an investigating authority rather than a prosecutor (*Murphy v Flood* [1999] IEHC 9).

For the purposes of conducting its investigations, the CAB has many of the powers normally given to *An Garda Síochána*, including search warrants and orders to make material available to the CAB. In addition, the CAB enjoys extensive powers of seizure in respect of assets which are the proceeds of crime and can apply *ex parte* to the High Court for short-term 'interim' orders on the civil standard of proof prohibiting a person from dealing with a specific asset (Section 2 of the Proceeds of Crime Act 1996). Section 3 allows for the longer-term freezing of assets ('an interlocutory order'), for a minimum of seven years. At the expiry of seven years, the CAB can apply to transfer the asset in question to the Minister for Public Expenditure & Reform or other such persons as the court may determine.

The courts have treated bitcoin as an asset capable of recovery under the CAB's powers and have not distinguished virtual currencies from other assets for this purpose (*Criminal Assets Bureau v Mannion* [2018] IEHC 729).

Reporting obligations

Uncovering wrongdoing in the course of an internal investigation may give rise to a statutory reporting obligation. It is an offence under Section 19 of the Criminal Justice Act 2011 to fail, without reasonable excuse, to notify the appropriate authority where a 'designated person' has information which they know or believe to be of material assistance in preventing the commission, or in securing the successful prosecution, of a relevant offence. 'Relevant offences' include: criminal damage; fraud; bribery; theft; company law violations; and offences relating to the investment of funds and other financial activities. The threshold is low and need not meet an evidential standard. Designated persons must be alert to this obligation as any failure to comply carries the risk of a substantial fine on conviction for individuals and entities, and/or a term of imprisonment of up to five years for relevant individuals.

A Section 19 report can be made orally but is best submitted in writing, a copy of which should be retained as a written record of the notification so that the extent/timing of the report is evident in the event of any subsequent attempt to prosecute the designated person.

Where money laundering is suspected, care must be taken to notify and to seek directions from the authorities as to the steps that the individual or entity must take in connection with the resulting criminal investigation. Tipping off in respect of money laundering is an offence.

Auditors also have strict reporting obligations under Section 59 of the Criminal Justice (Theft & Fraud Offences) Act 2001 if information of which the auditor may become aware in the course of an audit suggests that the audited entity may have committed offences of dishonesty.

Whistleblowers

Whistleblowing reports are a common feature in the context of investigations and litigation. The enhanced protection for whistleblowers under the Protected Disclosures Act 2014 aims to encourage disclosure of potential wrongdoing. The legislation gives no guidance as to how disclosures are to be investigated, but care should be taken to retain confidentiality and to avoid any

steps which may be construed as penalisation of the discloser. The potential exposure to damages for breaches of the Act is very significant.

Legal privilege

Irish law recognises legal professional privilege as a fundamental doctrine, grounded on the public policy that an individual or entity can consult lawyers and prepare for litigation in confidence. Three primary sub-classes of privilege protect communications: those evidencing legal advice (*legal advice* privilege); generated for the dominant purpose of existing or contemplated litigation or regulatory investigations (*litigation* privilege); or evidencing settlement negotiations (*without prejudice* privilege). A document may be either fully or partly privileged. Privilege confers an absolute immunity from production and inspection, but may be tested once asserted. A party making discovery must list on oath each individual document over which privilege is claimed.

Privilege may be waived voluntarily or if privileged documents are deployed in the course of proceedings and the benefit of privilege is generally lost once shared with a third party; although there is a mechanism for protection of privilege where privileged documents are shared confidentially for a defined purpose, on the express understanding that privilege is not waived. Reliance on certain privileged documents may result in broader waiver of privilege. Privilege may also be forfeited if it can be established that the author/creator of the documents did so for the purposes of engaging in a fraud or other illegal conduct.

Administration of justice in public

The Irish Constitution provides that justice shall be administered in public save in such special cases as may be prescribed by law (Article 34(1) of Bunreacht na hÉireann). This constitutional imperative of open justice means that hearings do not take place in chambers, and there is no precedent for the granting of gagging orders in the context of the making of orders for disclosure, for example. A recent decision of the Supreme Court may open up scope for the granting of such orders in an appropriate case. In *Sunday Newspapers Ltd. & Ors. v Gilchrist and Rogers* [2017] IESC 18, the Supreme Court considered whether a defamation action before a jury, involving highly sensitive evidence affecting a state witness protection programme, could be heard *in camera*. Finding it could on the facts, the Court said that any court must be resolutely sceptical of any claim to depart from the general principle of open justice, but where constitutional interests and values of considerable weight may be damaged or destroyed by a hearing in public, then the minimum possible restrictions can be imposed to protect those interests. This opens up the possibility of obtaining reporting restrictions in the context of an application for disclosure by way of injunctive relief, where publicity may place the information at risk of destruction.

Data protection

Data protection in Ireland is governed by the Data Protection Acts 1988 to 2018 and the GDPR, which impose a range of obligations on 'data controllers' and 'data processors' as regards how they manage the 'personal data' of EU 'data subjects'. The definition of personal data is much broader than that applicable in the US, for example, and care must be taken to ensure that international transfers of such personal data meet the requirements of the GDPR.

There is a preliminary obligation on all data controllers/processors to identify at least one of the prescribed 'legitimate grounds' permitting the lawful collection and processing of personal data. Personal data must always be relevant to the purpose for which it is collected/processed. It should also be retained only for as long as is necessary for the purpose(s) for which it was originally collected and always properly secured against unauthorised access.

Data protection should always be a central consideration, particularly where, for example, a company requires access to the personal data of clients, employees or other third-party stakeholders as part of an internal investigation/audit or an external request from a third party (e.g. a regulator/investigative body). In most cases, data controllers/processors are required to first obtain either the express or implied consent of data subjects before collecting/processing their personal data, especially sensitive personal data which in virtually all cases requires express consent. Where, for example, a company is investigating a suspected fraud, one of a number of exceptions may apply permitting the requisite processing for the purpose of obtaining legal advice in connection with anticipated legal proceedings, or for the purposes of preventing, detecting or investigating suspected offences. For non-sensitive personal data, processing is generally permitted to the extent that it is incidental to and necessary for the pursuit of a company's 'legitimate interests' (e.g. compliance with the terms of an employment contract or protection of its commercial/financial interests) provided that this is done fairly and proportionately. The key questions are likely to be whether the intrusion is proportionate to the need and to what extent the information needs to be disclosed to anyone other than the investigator.

The Irish Data Protection Commissioner (DPC) is considered the lead supervisory authority in the EU due to the number of digital content providers domiciled in Ireland. Any breaches are required to be notified within 72 hours (where feasible) and it may also be necessary to notify those data subjects affected.

Constitutional privacy rights also underpin data protection law in Ireland. Privacy is recognised as an unenumerated right protected under the Irish Constitution and the potential for breaches of constitutional rights should also be borne in mind when handling personal data, conducting investigations or engaging in measures such as surreptitious monitoring, filming, or other intrusive conduct as part of any investigation or in the course of proceedings.

Breach of confidence

Claims for breach of confidence tend to arise in commercial contexts arising from the commercial exploitation of confidential information whereby a company, for example, might sue in respect of confidentiality obligations owed to it by third parties (e.g. (former) employees, clients, or other stakeholders). Companies routinely rely on the law of confidence in connection with the removal or disclosure of commercially sensitive information by an employee. Breach of confidence has a broader remit than data protection law as it applies to all information whether or not it constitutes 'personal data'. The information must be confidential and the party possessing it must have shared it in circumstances which impute a duty of confidentiality.

A company may also be sued in respect of confidentiality obligations owed by it to third parties (e.g. (former) employees, clients, or other stakeholders). Compliance with data protection law is also likely to satisfy the company's obligations in respect of confidentiality. Where a company feels that it is necessary to disclose confidential information received from a third party to parties other than public law enforcement authorities, it should, where possible, seek the consent of the party from whom it received the information.

Seeking/compelling disclosure from third parties

Irish law provides a number of mechanisms for obtaining disclosure from third parties either in the context of existing proceedings, or in aid of foreign proceedings, or with a view to commencing proceedings.

The court will grant orders for production of documents by a non-party if satisfied that it likely holds the documents and that they are relevant and necessary and not otherwise obtainable by the applicant, subject to the applicant indemnifying the non-party in respect of the reasonable costs of making discovery. The court will generally not make such orders against entities or individuals outside the jurisdiction, although such orders may be made with the consent of the affected non-party (*Quinn & Ors. v Wallace & Ors.* [2012] IEHC 334).

A party can also apply for the disclosure of information (see Order 40 of the Rules of the Superior Court (RSC) for details of the procedural requirements relating to sworn affidavit evidence) by a non-party where such information is not reasonably available to the requesting party provided that the court is satisfied that this information would not have been otherwise obtainable. The court may, unless it is satisfied that it would not be in the interests of justice that the subject matter be disclosed, grant an order on notice to the non-party directing them to: (i) prepare/file a document documenting the information; and (ii) serve a copy of that document on the parties to

the proceedings (Order 31, Rules of the Superior Courts (RSC) (as amended)).

Preservation of assets/documents

The courts will make orders for disclosure of documents as part of measures to restrain the dissipation of assets (*Irish Bank Resolution Corporation Ltd. (in Special Liquidation) & Ors. v Quinn & Ors.* [2013] IEHC 388; *Trafalgar Developments Ltd. & Ors. v Mazepin & Ors.* [2019] IEHC 7). Failure to comply with such orders constitutes a contempt of court, punishable by committal or attachment. The court will also take action to protect copyright by way of prior restraint in appropriate cases, for example (*EMI Records (Ireland) Ltd. v Eircom plc* [2009] IEHC 411).

Norwich Pharmacal orders

The courts will grant orders requiring the disclosure of information or documentation by a third party by way of *Norwich Pharmacal* relief in order to identify a wrongdoer (*Megaleasing UK Limited & Ors. v Barrett & Ors.* [1993] ILRM 497). In *easyJet plc v Model Communications Ltd* ([2011] (Unreported)), the easyJet board had been the subject of a viral social media campaign and sought *Norwich Pharmacal* relief against the Dublin-based PR company involved, which was ordered to produce its client's details and design materials, which confirmed that the originator of the campaign was a former shareholder of the company. Such orders are also frequently granted against internet service providers in respect of anonymous online content (see, for example, *McKeogh v John Doe 1 & Ors.* [2012] IEHC 95).

2 Case triage: main stages

When information about potential fraudulent activity emerges, careful consideration must be given to strategy and next steps. An internal investigation may lead to a disciplinary process, which may span different offices within an organisation and different jurisdictions, or give rise to mandatory reporting obligations. An organisation may be the victim of an external fraud or it may be a purely internal issue (or a hybrid of those scenarios). External investigations may result, with the organisation and its officers facing regulatory sanctions or criminal prosecution. Where this occurs, civil litigation is likely to arise or the organisation may need to pursue litigation to protect its own interests and that of any shareholders and to recover losses. It may be possible to contain the situation within the organisation or it may become public, and different considerations will apply depending on the circumstances but always with the possibility of reporting obligations informing next steps.

The process of planning and managing an internal investigation requires careful handling. Contractual considerations are key and the organisation must operate within the law. Contracts with officers and employees, as well as an organisation's internal codes and procedures, may include terms concerning the use of material that is protected by data protection law or that falls under separate confidentiality or privacy obligations. Even where there is no statutory requirement to report matters to the authorities, a decision may be made to do so voluntarily for internal policy reasons.

Documents, particularly electronic documents, should be immediately preserved. Depending on the purpose of an internal investigation, it may be possible to rely on legal professional privilege in respect of the communications and outputs from the process. If litigation is anticipated, a legal hold should issue to ensure preservation of relevant material.

A broad range of remedies is available to an organisation in tracing and recovering misappropriated assets depending on the circumstances of each case. Proving criminal fraud can be difficult, and it may be strategically more sensible to pursue alternative approaches to asset recovery *via* civil litigation.

When suspected fraudulent activity comes to light, an organisation should take immediate steps to investigate. Having preserved all relevant information, it may also be necessary to interview relevant personnel and/or secretly to view material stored on a personal computer or device, or hard copy documents located in an employee's office. An organisation must always have regard to its obligations to its employees, its customers and

other third-party stakeholders under data protection law and, separately, under confidentiality and privacy law. Many of these legal requirements may be satisfied by prior agreement between the organisation and the employee *via* a contract of employment, a separate non-disclosure agreement or relevant internal policy documentation. The organisation must also consider the extent to which it may be entitled to rely on legal professional privilege in respect of communications generated internally or with external lawyers, as well as the principles of procedural fairness that it must apply as regards the investigation process. If searches are to be conducted against personal data, a legitimate interest assessment should be conducted under GDPR prior to conducting any searches.

A further complicating factor in respect of internal investigations is that a protected disclosure may be made, sometimes by the person or persons under investigation. Where that occurs, considerable care should be taken to ensure compliance with the requirements of the Protected Disclosures Act 2014.

Remedies

There are various remedies available to organisations in Ireland in tracing/recovering misappropriated assets. These include:

Injunctive relief

The Irish courts have broad jurisdiction to grant injunctive relief in appropriate cases where damages are not an adequate remedy and where the applicant satisfies the court that the relief sought is necessary. In urgent cases, the courts may grant temporary orders (i.e. interim relief) without notice to the other side, but the applicant must make full and frank disclosure of all relevant facts and circumstances, and any failure to do so may lead to the relief being set aside and potentially to liability for damages.

Proceedings in general in Ireland are in open court and this should be borne in mind if seeking some of the remedies listed below given the risk of tipping off the other side.

Mareva injunctions

If the claimant is not claiming that it is entitled to some form of ownership of assets in the defendant's possession, but that it is unlikely to be able to recover funds from the defendant without a freezing order in respect of assets, then the freezing order sought is what is referred to as a Mareva injunction. A Mareva injunction can be a valuable pre-emptive remedy. It "*affects the assets of the party against whom it is granted, so as to prevent that party from placing such assets (save for assets in excess of any value threshold specified in in the relevant order) beyond the reach of the court in the event of a successful action*" (*Dowley v O'Brien* [2009] IEHC 566 at 760 per Clarke J). Given their nature, Mareva injunctions are often granted *ex parte*.

Ancillary orders in support of Mareva injunctions

Mareva injunctions are often accompanied by ancillary orders to ensure their efficacy, including Asset Disclosure Orders (*Trafalgar Developments Ltd. v Mazepin & Ors.* [2019] IEHC 7), aimed at ensuring defendants fully and accurately disclose the true extent of their assets, wherever situate, and/or orders for the cross-examination of a deponent on disclosure. The High Court in *AIB plc v McQuaid* ([2018] IEHC 516) invoked its inherent jurisdiction to join non-parties to proceedings to enforce its own processes/orders. There was no requirement for any substantive cause of action to subsist against the non-parties.

Anton Piller orders

Where there is an urgent fear that the respondent may try to move assets or hide evidence of wrongdoing, the courts may also grant search orders permitting the applicant to enter premises to look for evidence of wrongdoing and to demand information from named people about the whereabouts of assets ("Anton Piller orders"). The jurisdiction is "*sparingly used*" (see Section 1, Legal framework and statutory underpinnings). The courts may, in conjunction with freezing orders, order a respondent to disclose the whereabouts of assets in the respondent's possession identified as being 'stolen' assets or traceable back to such assets, or of the extent and whereabouts of assets that may need to be frozen so there are funds available to meet the claim.

Norwich Pharmacal orders

See Section 1, Legal framework and statutory underpinnings.

Bayer orders

In "*exceptional and compelling circumstances*" (*O'Neill v O'Keeffe* [2002] 2 IR 1), the court may restrain a respondent from leaving the jurisdiction for a limited time period and compel delivery of passports. Such orders are extremely rare and the court will qualify the restrictions as far as possible so as to balance the necessity for the proper administration of justice with the defendant's constitutional right to travel (*JN and C Ltd. v TK and JS trading as MI and LTB* [2002] IEHC 16).

Appointment of a receiver by the court

The aim of appointing a receiver before judgment is to preserve assets for the person who may ultimately be found to be entitled to those assets. The appointment of a receiver can be effective but is also an expensive and intrusive remedy. The appointment may occur in conjunction with other relief such as a Mareva injunction if there is, for example, a risk that a defendant may use a complicated structure to deal with their assets in breach of the injunction. This power is not limited to Irish-based assets. In the Quinn Family Litigation (*Irish Bank Resolution Corporation Ltd. (in Special Liquidation) & Ors. v Quinn & Ors.* [2012] IEHC 507), Ireland's specialised Commercial Court appointed a receiver over the personal assets of individual family members and later went so far as to appoint an Irish receiver over shares held by a UAE entity in an Indian company.

Where necessary the court will appoint a receiver over future income receipts derived from a defined asset in post-judgment scenarios (*ACC Loan Management Ltd. v Rickard* [2017] IECA 245).

Orders for the detention, preservation and sale of property

In addition to the inherent jurisdiction of the court under Section 28(8) of the Supreme Court of Judicature Act (Ireland), 1877 to grant relief, Order 50 of the Rules of the Superior Courts (RSC) provides for the detention, interim custody, preservation, securing and sale of property. Some of its rules apply to property that are the subject matter of proceedings and some apply more broadly to also include property that may be the subject of evidence given in proceedings.

European Account Preservation Orders (EAPO)

The European Account Preservation Order (EAPO), applicable since January 2017, has been little used. An EAPO is a bank account preservation order that exists alongside national preservation measures (Recital 6 of the EAPO Regulation 2014) and it prevents the transfer or withdrawal of funds up to the amount specified in the order which are held by a debtor or on their behalf in a bank account in a participating member state. It also enables the identification of relevant bank accounts by a simple online application procedure.

3 Parallel proceedings: A combined civil and criminal approach

It is possible to pursue civil and criminal proceedings on a parallel basis in Ireland, as occurs in civil law jurisdictions, although criminal proceedings may significantly delay the ability to obtain civil remedies. Private prosecutions are not a feature of Irish asset recovery because the Director of Public Prosecutions (DPP) has the option as to whether to prosecute where a private prosecution has been commenced and effectively takes over the prosecution. In general, civil proceedings are speedier and more effective than the criminal route. Note that where criminal proceedings do arise in respect of factual matters also arising in related civil proceedings, the courts may place a stay on the civil claim until the criminal trial has concluded if there is potential for prejudice to the accused. If stolen assets are involved it may be possible to involve the CAB.

Principal causes of action

Where a claimant has been the victim of a suspected fraud, careful consideration must be given to the nature of any proceedings that can or should be brought with a view to either recovering the assets or obtaining compensation commensurate with their value. Depending on

the facts, it may be possible to show that more than one party conspired in furtherance of the fraud such as to form the basis for a conspiracy claim; there may have been a (fraudulent) misrepresentation; it may be possible to show wilful deceit or unlawful interference with the claimant's economic interests or property; or there may be grounds to seek to rescind a contract on grounds of illegality. Where it is not possible to prove fraud, there may still be the option of an action for money had and received, provided that the claimant can identify the funds and demonstrate ownership of them, or for a garnishee order, for example.

Standard of proof

The standard of proof is the civil standard, i.e. the balance of probabilities (*Banco Ambrosiano SPA & Ors. v Ansbacher & Co. Ltd. & Ors.* [1987] ILRM 669), but the gravity of an allegation and the consequences of finding that it has been established are matters to which the court must have regard in applying the civil standard (*Fyffes plc v DCC plc & Ors.* [2005] IEHC 477). Counsel should not plead fraud unless satisfied that there are cogent grounds on which to do so and it is not permissible to allege fraud in vague or general terms. There must be evidence of conscious and deliberate dishonesty, and the plaintiff must be able to show that it has suffered a loss as a result of the fraudulent conduct.

Conspiracy

As with an allegation of fraud or deceit, any conspiracy claim must be pleaded in detail, with particulars of the facts giving rise to the conspiracy to the extent that they are known. A claim of conspiracy will usually be combined with other causes of action where it can be shown that more than one actor was involved in the events leading to the loss to the claimant. As with torts generally, the claimant must be able to demonstrate a causal nexus between the conspiracy and the loss or damage sustained. It is, of course, in the very nature of a conspiracy that facts are often concealed, so it can be challenging to meet this standard.

4 Key challenges

Parallel civil-criminal proceedings

It is not possible to control whether criminal proceedings will impact on civil asset recovery proceedings and, as identified above, the party pursuing the claim may find that it is fixed with reporting obligations which will necessarily result in involvement by prosecuting authorities. In general, if a claim meets the Commercial Court criteria, it is possible to move civil proceedings with expedition and obtain effective remedies through seeking injunctive relief and appropriate orders. The more egregious the facts, the better from the perspective of obtaining the assistance of the courts.

Norwich Pharmacal relief – limitations

It is not possible to obtain *Norwich Pharmacal* orders for general information concerning a wrongdoer. The court will insist on the information required being specified very particularly and the courts in this respect take a much narrower view than the English court, for example; Lord Philips MR pointed out in *Ashworth Hospital Authority v MGN Ltd.* [2001] 1 All ER 991 at [57]: "The present trend is to extend rather than marginalised this area of law." If foreign proceedings are already in being, the better route may be to seek disclosure orders from the Irish court in aid of those proceedings, provided that it is possible to identify data or documents that are relevant and necessary for that purpose and in the possession or power of an Irish person or entity.

Obtaining and accessing personal data

Compliance with the stringent requirements of the GDPR can be challenging in the context of an internal investigation where there are no legal proceedings in being and searches must be conducted against personal data. The better the organisation's general compliance with the GDPR, the easier it will be to move quickly in such circumstances. It should also be borne in mind that the definition of what constitutes personal data under the GDPR is much broader than its equivalent in the US, for example, and certain other jurisdictions.

Third-party litigation funding not permissible

As matters stand, it remains unlawful under Irish law for a third party to fund litigation, with the ancient rules of maintenance and champerty still effective under the Maintenance and Embracery Act 1634. The Supreme Court has recently addressed this twice (*SPV Osus Ltd. v HSBC Institutional Trust Services (Ireland) Limited & Ors.* [2018] IESC 44; see also *Persona Digital Telephony Ltd. & Anor v Minister for Public Enterprise & Ors.* [2017] IESC 27), stating clearly that such funding remains unlawful without legislation to rectify the situation. This can be a significant barrier to obtaining relief from the courts and it is hoped that the legislature will bring Ireland into line with other common law jurisdictions in this regard.

5 Cross-jurisdictional mechanisms: Recent issues and solutions

Misappropriated assets are often hidden across national borders and require international cooperation in order to be traced properly. The Irish courts have proved to be pragmatic and responsive in the recognition of judgments and other steps which will assist the tracing of assets cross-jurisdictionally.

This pragmatism can be illustrated by reference to a bankruptcy case arising out of the financial crisis (*Re: Drumm (a Bankrupt): Dwyer, applicant* [2010] IEHC 546). The bankrupt was the former CEO of the now notorious Anglo Irish Bank Corporation. The bank sued him for repayment of substantial share loans extended to him as CEO and in respect of the alleged fraudulent transfer of a property into his wife's name. He filed for bankruptcy in Massachusetts just prior to the hearing of the Irish High Court proceedings. The Trustee in bankruptcy applied to the Irish Court for orders in aid of the US bankruptcy proceedings vesting the property in the Trustee, assisting in the realisation of any other assets and in the examination of the bankrupt in respect of all matters relating to his estate. Ms. Justice Dunne noted that there was a paucity of decisions on point. She concluded:

"*We do live in a world of increasing world trade and globalisation... Whether one is talking of companies trading internationally or of individuals who have establishments in more than one jurisdiction, the fact of the matter is that businesses and individuals are infinitely more mobile than was the case in 1770. I can see no reason of public policy for refusing to assist the trustee in bankruptcy in this case in the manner sought. On the contrary, it seems to me that it is to the benefit of the creditors of the bankrupt to facilitate the trustee in this case. One of the principal creditors of the bankrupt is Anglo Irish Bank Corporation Plc which is participating in the bankruptcy proceedings in the United States of America. There is no obvious disadvantage to the creditors in refusing to make an order in aid of the trustee in bankruptcy and on a practical basis, it would appear to be more appropriate to make such an order so that the property in this jurisdiction can be dealt with by the trustee in bankruptcy for the benefit of all of the creditors of the bankrupt.*"

Letters of request

Letters of Request are a cross-jurisdictional mechanism whereby a court in e.g. Ireland can request assistance from a court in another jurisdiction in obtaining documents and/or evidence, in support of proceedings.

Letters of Request are a very effective cross-jurisdictional mechanism and have been used to great effect in the context of Irish conspiracy proceedings, in which neighbouring courts issued Letters of Request to the courts in Belize and the British Virgin Islands for assistance, resulting in the appointment of a receiver and the ultimate recovery of substantial assets (*Irish Bank Resolution Corporation Ltd. (in Special Liquidation) & Ors. v Quinn & Ors.* [2013] IEHC 388). The Evidence Regulation (Council Regulation (EC) No 1206/2001 of 28 May 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters (OJ L 174, 27.6.2001, p. 1)) applies in an EU context.

Enforcement of judgments

The Irish courts' attitude to the enforcement of foreign judgments is positive and facilitative. The enforcement of EU judgments is governed by the Brussels I Recast Regulation in respect of judgments or proceedings commenced after 10 January 2015; the Brussels I Regulation (44/2001) continues to apply to certain territories of Member States situate outside the EU. Ireland is also a party to the Lugano Convention 2007, relevant to certain EFTA Member States, and expects to be a party to the Hague Convention on the Recognition and Enforcement of Foreign Judgments in Civil or Commercial Matters 2019, both by virtue of its EU membership.

In respect of third-country judgments there are several multilateral treaties relevant to the recognition and enforcement of foreign judgments in Ireland. Only money judgments may be recognised and enforced at common law in Ireland and a party will generally apply for both recognition and execution if seeking the assistance of the Irish court. On the basis of respect and comity between international courts, provided the judgment is for a definite sum, is final and conclusive, and has been given by a court of competent jurisdiction, the court will generally recognise the judgment.

Grounds on which recognition and enforcement of such judgments may be refused include if Ireland is not considered to be the appropriate jurisdiction for recognition, if it is contrary to public policy, if the sums claimed have not been specifically determined, or if the court granting the judgment was not a court of competent jurisdiction (*Albaniabeg Ambient ShpK v Enel SpA* (2016) IEHC 139 and (2018) IECA 46; see also *Sporting Index Ltd. v O'Shea* (2015) IEHC 407).

Appointment of a receiver

The appointment of a receiver is also an effective cross-jurisdictional mechanism. (See also Section 2, Case triage: main stages, remedies.)

6 Technological advancements and their influence

Technology is a key tool in asset recovery and machine learning systems are commonly now deployed in fraud and asset recovery litigation in Ireland both in terms of tracing assets and also managing the complex discovery exercises which tend to accompany such disputes. The Irish courts have been particularly progressive in this regard, and Ireland was the second jurisdiction globally to approve the use of technology assisted review for making discovery (*Irish Bank Resolution Corporation Ltd. (in Special Liquidation) & Ors. v Quinn & Ors.* [2013] IEHC 388). Ireland's Chief Justice is seeking to introduce technology more broadly in the courts system and it is common for documents to be presented electronically in complex litigation.

There is an emerging trend of international investigators seeking to promote intelligence software for asset recovery. As GDPR compliance is central to the effective deployment of such technology, data protection obligations must be the first port of call in assessing to what extent intelligence systems are likely to validly advance the asset recovery efforts without giving rise to data protection breaches, a consideration which comes into stark focus when dealing with cross-border asset recovery given the divergent data protection regimes in different jurisdictions and differing notions of data protection globally.

There is no doubt that the Irish courts view bitcoin and other virtual currencies as 'assets' and the Commercial Court has granted freezing orders in respect of cryptocurrency, including digital wallets: *Trafalgar Developments Ltd. & Ors. v Mazepin & Ors.* [2019] IEHC 7. The CAB has also been granted orders entitling it to seize bitcoin. We expect to see an increase in disputes involving virtual currencies as uptake increases in Ireland following the implementation of MLD5, which for the first time regulates providers engaged in exchange services between virtual and fiat currencies and custodian wallet providers which will be subject to registration and due diligence requirements.

7 Recent developments and other impacting factors

MLD5

MLD5 changes the regulatory landscape across the EU in respect of virtual currencies and its implementation is a significant new development, as central banks struggle with the status and impact of such currencies. With moves by global companies such as Facebook towards setting up their own digital currencies, Ireland is at the centre of this new regulatory regime and is likely to see related litigation in the years to come. Ireland's unique legal system, with its important constitutional backdrop which is very focused on vindicating the rights of the citizen, may give rise to some interesting precedents in this area.

Brexit

It is impossible to provide any analysis of the legal framework and environment in Ireland in 2020

without mentioning the departure of the UK from the EU, otherwise known as 'Brexit'. Ireland will be uniquely impacted by Brexit being the only member state to share a land border with the UK and it appears that the ongoing constitutional crisis as regards the status of Scotland and Northern Ireland, neither of which voted to leave the EU, is likely to play out for some time to come. From the perspective of litigating in Ireland, the nature of the trade deal that is ultimately struck as between the UK and EU is potentially significant, because the UK appears at present to favour a level of divergence from EU law that is likely to interfere with asset recovery efforts involving parties in the UK, Ireland and other member states. Divergences in data protection laws are likely to have a significant impact on such litigation, given the stringent requirements of the GDPR and the difficult hurdles involved in transferring personal data to a third country. While it seems wildly counter-intuitive from an Irish perspective to leave the well-developed and highly efficient reciprocal mechanisms for recognition of judgments and other regimes, such as the European Arrest Warrant, the detail of the trade deal could really impact cross-border litigation.

Karyn Harty is an expert in asset recovery and fraud litigation. She has an in-depth knowledge of working with counsel in other jurisdictions, including civil law countries, as lead counsel, and securing orders and necessary sanctions in support of asset tracing including injunctions, the appointment of receivers and liquidators, findings of contempt of court, freezing orders and disclosure orders.

Karyn is Co-Chair of the Forum on the International Enforcement of Judgments and Awards 2019/2020 and is a regular contributor to conferences on international disputes and asset recovery.

Karyn is well known as an e-discovery specialist and secured the first High Court approval for the use of Technology Assisted Review in inter party discovery. Karyn has specialised in media defence since qualifying and she is supported by a team of media defence specialists who focus on complex media litigation, involving defamation, breach of confidence, contempt of court, privacy and injunctions.

karyn.harty@mccannfitzgerald.com

Audrey Byrne is an intelligent litigator and strategist who brings clear vision to the most complex of legal problems. Her practice focuses on complex commercial and taxation disputes and investigations, with a particular focus on international asset tracing, fraud and investigations. She frequently advises international clients (including foreign law firms) on cross-border issues and has a particular interest in white-collar crime compliance and contentious issues.

Audrey has unique experience in the Irish market of co-ordinating international litigation including fraud and asset tracing across multiple jurisdictions. Allied to this, she has extensive experience in dealing with regulatory bodies such as the Garda Bureau of Fraud Investigation and the Office of the Director of Corporate Enforcement.

audrey.byrne@mccannfitzgerald.com

Japan

Hiroyuki Kanae
Anderson Mōri & Tomotsune

Hidetaka Miyake
Anderson Mōri & Tomotsune

Atsushi Nishitani
Anderson Mōri & Tomotsune

1 Important legal framework and static underpinnings to fraud, asset tracing and recovery schemes

Japanese civil law permits the filing of an action for damages caused by fraud or tort, and provides a mechanism to enforce compulsory execution against the property of the wrongdoer based on a successful final and binding judgment. However, the legal proceedings could take a considerable amount of time, during which the assets of the defendant could be drained before compulsory execution could be carried out upon receipt of a favourable judgment. Therefore, preservation procedures, such as provisional seizure and provisional disposition, exist as a means to preserve the property of the wrongdoer and to prevent the dispersion and dissipation of that property.

1.1 Attachment

Attachment is recognised as a means to maintain the current status of property and to preserve that property for future compulsory execution, and may be allowed on selected appropriate property corresponding to the amount of a monetary claim from among the non-exempt property of the debtor that is the subject of the execution. When money is the subject of a fraud, it can be difficult to determine the location of that money. However, if, for example, the fraudulent act was a request to transfer money to a specific bank account, a claimant may be able to obtain a provisional attachment order and request that the bank account be frozen. Banks generally will not freeze their deposits without an attachment order issued by a court, so the attachment procedure should be followed.

1.2 Provisional injunction order

The provisional injunction order procedure is used to maintain the *status quo* of a specific property when a creditor has a claim against the debtor for that specific property, and when any change in the current physical or legal status of the property is likely to make it impossible or extremely difficult to enforce the claim in the future.

1.3 Requirements for preservation procedures

Preservation procedures require a *prima facie* showing of the existence of a right to be preserved. For example, attachment only applies to a claim for the payment of money. The existence of a claim for the payment of money will be obvious in cases of fraud and other illegal activities seeking recovery of money or property having value. However, a *prima facie* case of fraud requires a factual showing, for example, that the property invested by a creditor was not actually used for any intended investment or that the investment itself was fictitious. As an example, an individual solicited investments in a medical collections business, MRI International, Inc., but did not use the invested funds for the intended investment purposes. Further, a company, World Ocean Farm, raised funds for the purpose of investing in shrimp farming in the Philippines, but did not undertake any actual investment activity as described in the fund-raising plan. In both cases, individuals were found liable for fraud.

In addition, attachment is appropriate when there is a likelihood that compulsory execution will not be possible or when significant difficulties will arise in implementing compulsory execution. The need for preservation will generally occur in cases in which there is a risk that the debtor's culpable assets could be quantitatively and qualitatively reduced due to destruction, waste, resale, concealment, or expropriation, or where the debtor's culpable assets would become unsuitable if sold in the form of disposition of real estate, or where it would be difficult to ascertain the debtor's culpable assets due to the debtor's escape or relocation.

1.4 Protection measures for debtors

In attachment proceedings, a temporary restraining order may be issued against the debtor based on a creditor's unilateral claim or based on a *prima facie* showing, which may avoid full confirmation of the claim. The issuance of a temporary restraining order may be a decisive blow to the debtor, so the court may require a security deposit from the creditor to protect against damage that the debtor may incur to preserve the civil claim. The existence of a claim is relatively clear in the case of a loan claim or a receivable arising from a sales contract. However, the existence of a claim is not necessarily clear in the case of a claim for damages arising from a tort, such as fraud. Accordingly, the security deposit for an order of provisional seizure, in which the claim for damages caused by a tort is a secured claim, is often made on the condition that a statutory bond of at least 30% of the claim is deposited with the relevant Legal Affairs Bureau. Thus, the preservation procedure and the subsequent proceedings require a considerable amount of funds.

2 Compulsory execution procedure after obtaining a judgment in a civil suit

A plaintiff (creditor) who has prevailed on a fraud claim in a civil suit may seize the real estate, personal property, bank deposits, and other monetary assets held by the defendant (debtor). In the case of a monetary claim for fraud, a declaration of provisional execution is usually attached to the judgment of the first instance, and therefore, it is possible to seize the defendant's property even before the judgment becomes final and binding. In those circumstances, if a provisional seizure order is obtained and placed on the defendant's property at an early stage, effective compulsory execution is possible because the property will be preserved. In the case of a tort claim, it is usually difficult to apply for compulsory execution against the defendant's property after obtaining a judgment.

2.1 Property disclosure order

The Civil Execution Law provides for an order requiring a debtor to disclose his/her assets. If the debtor violates the property disclosure order, he/she is subject to a fine. In practical terms, a property disclosure order is aimed at collecting claims using the pressure of the imposition of fines. Requirements for an order for the disclosure of property are as follows.

A creditor of a monetary claim who has an enforceable authenticated copy of a title of obligation may file a petition for an order requiring the debtor to disclose property when the creditor has made a *prima facie* showing that the debtor has been unable to receive full performance under the monetary claim or when the creditor has made a *prima facie* showing that he/she is unable to obtain full performance under the monetary claim even by implementing compulsory execution against known property (Article

197 of the Civil Execution Law). Courts may prescribe a deadline for disclosure of information and impose an obligation on the debtor to make statements concerning his/her property (Article 197 of the Act). Failure to comply with a disclosure order by the court-imposed deadline without a reasonable basis to do so or without a sworn statement, or provision of a false statement in a sworn disclosure is punishable by imprisonment with work for not more than six months or a fine of not more than 500,000 yen (Article 213 of the Act). In practice, effective collection of monetary claims is often made by stressing the possibility of a petition for a property disclosure order and criminal sanctions.

3 Bankruptcy petition

If a debtor does not make any payment toward a final and binding judgment, a judgment creditor may file a petition for the adjudication of bankruptcy against the debtor based on the creditor's claim. Upon rendering an adjudication order, a court-appointed trustee will have the power to investigate the debtor's property. If a debtor makes a false statement in connection with the investigation, the debtor would be in violation of bankruptcy law and would be subject to criminal punishment, which could be a powerful tool for collecting claims.

4 Case triage: main stage of fraud, assets tracing and recovery cases

As described above, if a plaintiff obtains a favourable judgment in a civil suit, the defendant's deposit account or other property may be subject to compulsory execution, and property may be seized. However, the location of a defendant's property may be impossible to ascertain, so it is important to initiate attachment or provisional injunction procedures against known property before filing a lawsuit.

4.1 Filing of a criminal complaint

A creditor must bear the legal costs incurred in bringing an action and obtaining judgment and compulsory execution. Therefore, in order to clarify the actual situation through investigation by the authorities, a creditor may commonly file a criminal complaint with the police to urge the authorities to investigate and to recover damages by having the police or the public prosecutor confiscate the property during the criminal procedure process.

If an investigation reveals fraud has been committed in violation of the Law on Punishment of Organized Crime, the investigating authorities may seize and confiscate funds collected by the criminal offender. Investigative bodies, such as the police and prosecutors, have the authority to compulsorily collect deposit information and other information from banks and other financial institutions, and thus, can arrest and prosecute criminal offenders, and confiscate property, when the evidence of fraud is clear.

In particular, the Law on Punishment of Organized Crime provides for the confiscation and collection of property derived from organised crime. Organised crime pursuant to this law includes not only illegal transactions, such as the sale of narcotics, but also organised fraud, such as solicitation and execution of fictitious investments, either inside or outside of Japan. Thus, in addition to seeking criminal prosecution of the offender who engaged in fraudulent solicitation, the investigative authorities may confiscate the proceeds from illegal acts. In addition, the investigating authorities may be required to distribute the proceeds based on the victim recovery benefit system.

Accordingly, recovery of overseas assets is difficult without the involvement of the law enforcement institutions. Therefore, if the whereabouts of foreign assets are known, it is important to prevent leakage of those assets by

first executing the procedures for attachment and provisional disposition of foreign assets in collaboration with overseas lawyers at an early stage. Therefore, building an international network of lawyers is recommended.

5 Case study

The World Ocean Farm case presents an example of international investment fraud. The wrongdoers stated that they ran a shrimp farm in the Philippines, the size of which was 450 times the width of Tokyo Dome. Potential investors were told that investments in the business would double in one year. Distribution of the investment funds was accomplished in the name of a limited liability partnership. The wrongdoers collected approximately 85 billion yen from about 35,000 people. The investment turned out to be a large-scale Ponzi scheme. More than 10 company executives involved in the fraud were arrested and indicted, and the former chairman was sentenced to 14 years in prison on fraud charges. Although the victims suffered considerable damages, the Ponzi scheme left no significant property in Japan, and $40 million that had been concealed in United States financial institutions for money laundering was seized by the FBI. The Japanese and United States authorities negotiated the return of the seized funds, and a fund of $40,269,890 was returned to the victims (http://justice.gov/opa/pr/2010.May/10-crm-627.html).

For proceeds of organised crime, a framework of procedures, such as confiscation and return, within the international legal framework, such as the International Criminal Proceeds Transfer Prevention Act, is indispensable for recovery.

6 Parallel proceedings: a combined civil and criminal approach

6.1 Standard non-parallel approach

In Japan, a combined civil and criminal approach is not often seen in practice, and there are few cases in which criminal and civil procedures are used concurrently to recover damages caused by fraud. Notably, there are no discovery procedures in civil proceedings in Japan. Thus, every plaintiff must individually collect evidence to prove fraud, and it is generally difficult to collect sufficient evidence to obtain a favourable civil judgement. Therefore, in many cases, a victim will file a complaint with law enforcement authorities before initiating a civil lawsuit, expecting that the whole picture of fraud will be revealed by the investigation by the authorities. In the meantime, a wrongdoer often reaches a settlement with the victim(s), and the damages caused by fraud are recovered through the wrongdoer's performance of obligations contained in the settlement.

In the case of corporate insider fraud, such as embezzlement of corporate assets by an officer or employee of a company, the company may be able to collect a considerable amount of evidence successfully by conducting an internal or independent fraud investigation. Even in such case, however, the company will often negotiate with the wrongdoer in an effort to recover the damages before filing a complaint with law enforcement authorities, and will determine whether to file a complaint with law enforcement authorities taking into account the status of voluntary damage recovery by the wrongdoer. If the public prosecutor or the police have already received a criminal complaint and commenced an investigation, the public prosecutor may drop the case if the criminal suspect and the victim(s) reach a settlement. Even after an investigation and an indictment, the public prosecutor may request a less severe penalty from the court if the defendant and the victim(s) reach a settlement.

A wrongdoer may be able to avoid criminal charges or a severe criminal penalty by reaching a settlement with victim(s). As such, it is often seen in practice that victim(s) recover consider-

able damages through out-of-court settlements in criminal proceedings.

7 Restitution court order

A restitution court order provides an approach similar to parallel criminal and civil proceedings in accordance with Chapter 7 of the Act on Measures Incidental to Criminal Procedures for Protecting Rights and Interests of Crime Victims. In this approach, a criminal court that has found a defendant guilty in a criminal trial continues to hear a claim for damages from victim(s), and may order the defendant to compensate the victim(s) for the damages. This proceeding resolves the issue of damages recovery summarily and promptly. However, a restitution court order is available only in a criminal case in which a person is killed or injured by an intentional criminal act, such as murder, so it cannot be used to recover damages caused by property offences, such as fraud.

8 Remission payments using stolen and misappropriated property

A remission payment under the Act on Issuance of Remission Payments Using Stolen and Misappropriated Property can be used as a tool to recover damages caused by property offences, such as fraud. In particular, assets that have been confiscated (or property equivalent to the forcibly-collected value of stolen and misappropriated property) in criminal trials of certain crimes, such as organised crimes or black-market lending cases, are stored in monetary form, and remission payments are made to victims. In this process, the criminal proceedings precede the administrative procedures in which the public prosecutors carry out remission payments. Therefore, this is not a true combined civil and criminal approach, but it has the similar effect of quick damage recovery.

9 Damage recovery benefit distributed from fund in bank accounts used for crimes

The Act on Damage Recovery Benefit Distributed from Fund in Bank Accounts Used for Crimes provides procedures for distribution of recovered damages from bank accounts used in cases of bank transfer or similar fraud. In order to achieve damage recovery for victims of these types of fraud, the procedures enable a financial institution to distribute damage recovery benefits from funds that are deposited in a bank account of the financial institution used for the fraud. Thus, a financial institution, upon notification by a victim(s), may take certain measures, including suspension of transactions in the bank accounts. Claims on the bank account will be extinguished after a public notice by the Deposit Insurance Corporation, and the remaining funds in the deposit amount will be distributed to the victim(s) as damage recovery benefits. No civil action will be required except for certain cases in which a party makes a claim to the deposit account. In addition, criminal procedures will not be required in this process.

10 Key Challenges

As mentioned above, under the current legal system in Japan, the most effective way to determine the whole picture of fraud is to influence law enforcement authorities, such as the public prosecutor, the police, or the Securities and Exchange Surveillance Commission, to commence governmental investigations. In practice, however, law enforcement officers will not officially accept a complaint from a victim unless the victim presents strong evidence to support the fraud allegations. Therefore, in the case of corporate insider fraud, such as those involving a company officer or employee, the company should conduct its own fraud investigation and collect strong evidence through in-depth investigative procedures, such as electronic data review, utilising digital forensics, in order to present evidence to law enforcement authorities.

In Japan, fraud investigations conducted by so-called "third-party committees" that are independent from a company have become common practice in corporate crisis management. However, in order to maintain the strict independence of third-party committees, the Japan Federation of Bar Associations has issued guidelines for practitioners of these committees that restrict the committee's ability to share its evidence with the company. Thus, even if a third-party committee obtains strong evidence to prove fraudulent acts, it will generally be difficult for the company to use that evidence in its other crisis management actions, such as taking disciplinary action or seeking compensation for damages against a wrongdoer. The key challenge for companies is to conduct an objective and independent fact-finding exercise while establishing appropriate investigative structures that enable the company to continue effective corporate crisis management activities.

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

In Japan, it is generally difficult in practice to recover assets concealed outside the territory of Japan without the involvement of governmental authorities.

The Act on Issuance of Remission Payments Using Stolen and Misappropriated Property sets out procedures for restoration payments using property transferred from abroad. Under those procedures, the Japanese government, under certain conditions, will restore the property subject to confiscation (or a collection of property of equivalent value) by a court or similar proceedings under the laws and regulations of a foreign country, and issue the restoration payments to a victim(s) using the property. In a famous black-market financing case by the *Goryokai* criminal organisation, the Japanese government restored property worth about 2.9 billion yen transferred from Switzerland where the state government confiscated the wrongdoer's property. Then, the amount of money corresponding to the amount of damage suffered by the victims was paid as restoration payments.

In a cross-border Ponzi scheme investment fraud by a United States-based asset manager, MRI International, the Financial Services Agency issued an administrative action, but Japanese law enforcement authorities did not launch a criminal investigation. Some of the victims filed a civil suit against MRI seeking payment of a maturity reimbursement. In 2014, the Tokyo District Court ruled that the provision in the contract establishing exclusive jurisdiction in the State of Nevada was valid. However, the appellate court ruled in 2014 that the exclusive jurisdiction clause was invalid, and the Supreme Court dismissed and rejected MRI's appeal in 2015, thus clearing the way for the victims to hold MRI responsible in a Japanese court. In the meantime, victims conducted concurrent class actions in the United States for recovery of damages.

12 Technological advances and their influences on fraud, asset tracing and recovery

In Japan, there have recently been two major incidents in the virtual currency (cryptographic asset) industry.

In the Mt. Gox incident, bitcoin worth about 48 billion yen was lost in February 2014. In the same month, Mt. Gox filed for bankruptcy. The company's president was later arrested and charged with embezzling customers' accounts. He was not found guilty of embezzlement, but he was sentenced to two years and six months in prison, which was suspended for four years, for creating and using false private electronic records. With regard to recovery of damages, the subsequent steep rise in bitcoin prices created an extremely unusual situation in which the bankruptcy proceedings of Mt. Gox were moved to civil rehabilitation proceedings. Victims (creditors) could recover damages in the form of divi-

dends in civil rehabilitation proceedings. In the wake of the Mt. Gox scandal, the Financial Services Agency revised the law to introduce a registration system for virtual currency exchange operators, putting them under the supervision of the authorities for the first time anywhere in the world.

In the Coincheck incident, about 58 billion yen worth of virtual currency NEM was leaked in January 2018. Coincheck put the "private key" used for transactions, such as remittance of virtual currency, in a so-called hot wallet connected to the Internet. (Note: A wallet disconnected from the net is called a cold wallet.) The private key was allegedly stolen by an outside hacker through the Internet, and a large number of NEMs were stolen. The NEM Foundation, in cooperation with engineers, placed tracking mosaics on the stolen NEM wallets, keeping them under constant surveillance to prevent perpetrators from converting the stolen NEM into other currencies. However, even with this tracking method, if the perpetrator exchanged the NEM for another currency in the highly anonymous network called the Dark Web, identification of the perpetrator who stole the NEM would be extremely difficult. Because hacking from overseas was also raised as a possibility, administrative supervision and legislation in Japan alone could not adequately deal with the incident. The Financial Stability Board, which comprises financial supervisory authorities in major countries, started creating a "contact list" to help local authorities in charge of virtual currency administration in each country understand their responsibilities. In addition, in the event that any cybercrime actually occurs, a system must be established to identify the culprit through international cooperation among investigative authorities and engineers in each country, and to investigate and recover assets outside Japan.

13 Recent developments and other impacting factors

In Japan, with the revision of the Code of Criminal Procedure in May 2016, a Japanese version of plea bargaining was introduced in June 2018. Plea bargaining made it possible for Japanese public prosecutors to agree with suspects and defendants on measures favourable to them, such as suspension of prosecution, prosecution for lighter offences, and a request for a summary order, in exchange for cooperation in criminal investigations (Article 350 (2) of the Code of Criminal Procedure).

Applicable crimes include not only organised crimes related to drugs and weapons, but also a wide range of economic crimes, such as fraud, embezzlement, bribery and cartels.

The Japanese version of plea bargaining is characterised not by self-incrimination, but by cooperation in investigations relating to "crimes committed by others". Even a declaration by a person or a corporation of his/her/its own crime does not, by itself, satisfy the requirements of plea bargaining under the law. Plea bargaining requires cooperation in an investigation, such as testifying about, and/or submitting evidence of, "crimes committed by others".

Plea bargaining has been used in three cases in Japan. The first case involved bribery of a foreign public official in connection with the construction of a power plant in Thailand (Violation of the Unfair Competition Prevention Act). The parties reached a plea agreement in July 2018, and as a result of cooperating in an investigation into a crime committed by a former executive, the company and local employees escaped prosecution.

The second case involved Nissan President Carlos Ghosn's fabrication of financial statements (Violations of the Financial Securities and Exchange Law) (judicial transaction closed around November 2018). Certain executives cooperated in the investigation of Ghosn's crime, and were exempted from prosecution while Carlos Ghosn and Nissan were prosecuted.

The third case involved embezzlement of company funds by a representative director of an apparel company. In November 2019, a special investigation squad of the Tokyo District Public Prosecutors Office reached a plea deal with an employee who was ordered to commit fraud.

Hiroyuki Kanae graduated from Waseda University School Law (1976), Legal Training Institute of the Supreme Court of Japan (1979) and the University of Illinois at Urbana Champaign, College of Law (1987). He is qualified in Japan (1976) and New York (1988). He has served as a corporate auditor of a premier international logistic company since 2012 and advises the management with the corporate governance and legal matters surrounding the international business. He focuses on commercial litigation matters, including domestic and cross-border litigations involving major Japanese and foreign companies. He has been advising on the global asset recovery projects involving Japanese clients in USA, Asia and Europe. He has represented trustees in bankruptcy proceedings in Japan, in pursuing successful asset recovery in the United States.

hiroyuki.kanae@amt-law.com

Hidetaka Miyake served as a public prosecutor from 2000 to 2004. After being admitted as a Japan qualified attorney in 2004, he experienced private practice at a UK law. From 2010 to 2013, he served as a senior securities investigator at the Securities and Exchange Surveillance Commission. From 2013 to 2017, he served as a senior manager in a forensic accounting team of a Big Four accounting firm. Since joining Anderson Mori & Tomotsune as an expert of crisis management in 2017, he has handled accounting fraud investigations for more than 10 Japanese listed companies. Since 2018, he has been advising a listed regional bank on crisis management and compliance issues in relation to its shared house loan scandal, which is one of the biggest recent corporate scandals in Japan.

hidetaka.miyake@amt-law.com

Atsushi Nishitani graduated from Tokyo University (1997), Legal Training Institute of the Supreme Court of Japan (2002) and University of California Berkeley School of Law (LL.M.) (2013). He is qualified as a lawyer in Japan (2002) and New York (2014), as well as a certified fraud examiner (2016). He handles crisis management and insolvency matters including cross-border cases with practical advice enhanced by his experience in Tokyo and New York at one of the largest Japanese trading corporations. Among his career, he has engaged in fraud investigation and asset tracing/recovery including financial frauds and quality-test frauds as a member of investigation committees established by Japanese listed corporations. He is also vastly experienced with cross-border crisis management matters such as a financial fraud in China and a bribery case in Indonesia which triggered the US Foreign Corrupt Practices Act of 1977 (FCPA).

atsushi.nishitani@amt-law.com

Anderson Mōri & Tomotsune is a full-service law firm formed by the winning combination of three leading law firms in Japan: Anderson Mōri, one of the largest international firms in Japan which was best known for serving overseas companies doing business in Japan since the early 1950s; Tomotsune & Kimura, particularly well-known for its expertise in international finance transactions; and Bingham Sakai Mimura Aizawa, a premier international insolvency/restructuring and crisis-management firm.

We are proud of our long tradition of serving the international business and legal communities and our reputation as one of the largest full-service law firms in Japan. Our combined expertise enables us to deliver comprehensive advice on virtually all legal issues that may arise from a corporate transaction. The majority of our lawyers are bi-lingual and experienced with communicating, drafting and negotiating across borders and around the globe. We welcome the opportunity to work closely with clients and channel our resources towards our goal of achieving more together.

www.amt-law.com

ANDERSON MŌRI & TOMOTSUNE

Luxembourg

Max Mailliet
E2M –
Etude Max Mailliet

Luxembourg, a country once known for its steel industry, has become an important worldwide financial centre, ranking among the top three EU financial centres; not bad for a country that has just over half a million inhabitants and where the capital city barely has 120,000 inhabitants overnight, which almost doubles during the day with workers streaming in from the countryside and neighbouring countries, Belgium, France and Germany.

Given the size and importance of the financial sector, the Luxembourg government and parliament have always endeavoured to keep the relevant legislation at a state-of-the-art level. As a result, and to the contrary of what is usually expressed by the public opinion, Luxembourg laws on money-laundering are extremely strict and the prosecution of criminal offences related to money-laundering is quite severe, especially with regard to non-compliance with AML regulations.

The official languages in Luxembourg are Luxembourgish (as a spoken language) and French and German as written/administrative languages. Judicial proceedings are usually conducted in French, but sometimes, oral arguments are also presented in Luxembourgish or German. Judgments are always written in French. Written evidence in English is becoming more and more accepted in Court proceedings, without the need for translation, but not in every Court.

Usually, fraud cases are pursued through civil litigation, rather than criminal, for reasons of speed and efficiency. It is not unusual to use insolvency as a tool in fraud cases, as it opens alternative routes for engaging liabilities and/or recovering assets.

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

A Framework for criminal proceeding

1 General considerations

The criminal legislation is based on the original French criminal code (the *code pénal* as Napoleon had it adopted) and violations of the criminal law are divided in three categories ranging from minor to criminal offences.

Since the law of 3 March 2010 on criminal liability of legal persons, legal persons such as companies are also criminally liable under Luxembourg law, this criminal liability applying to all types of criminal offences. In case a

company has been created for the sole purpose of committing a criminal offence or where, for certain specific offences, the company has been diverted from its object to commit the criminal offence, it may be dissolved by judgment of the criminal Courts.

Criminal proceedings are usually initiated by the State Prosecutor (*Procureur d'Etat*) either as a result of a criminal complaint, which has been filed with the State Prosecutor (*plainte pénale*) or with the Investigating Magistrate (*plainte pénale avec constitution de partie civile entre les mains du juge d'instruction*).

Such proceedings are very much in the hands of the authorities and the latter rarely take into account outside help. Access to the investigation files is also made as difficult as possible, as much for the perpetrators as for the victims. It is only when the investigation is at a very advanced stage that the victim and the perpetrator are granted access to the case file.

Furthermore, investigators rarely provide conclusive answers on the evolution of a case, as Luxembourg proceedings are subject to secrecy rules which are enforced quite tightly.

The State Prosecutor always has the right to decide whether prosecution is necessary and appropriate (*principe d'opportunité des poursuites*). However, if the State Prosecutor decides not to prosecute the case, this is not to be deemed as an acquittal, but simply an administrative decision. The victim, or any other third party which is able to prove that it has an interest to take action, can then still seize the criminal Courts directly, save for crimes.

The powers of the investigating authorities have become quite broad over the time, and, especially, the bank secrecy rules cannot be upheld towards the criminal authorities.

For certain specific offences, such as, for instance, money laundering, the Investigating Magistrate may further order a bank to inform them if a suspect has or controls any accounts with that bank or order a bank to inform them about all the operations conducted or planned. The Investigating Magistrate may further request mutual assistance in legal matters from foreign authorities.

At the beginning of an investigation, the Investigating Magistrate will usually freeze the bank accounts and assets, which appear to have a connection with the offence under investigation in that they are potentially subject to be proceeds of such offence. The victim or any third parties having a legitimate right on the frozen accounts may require from the Courts (the *Chambre du Conseil*) the lifting of the freezing order, bearing in mind that such liftings are rarely granted.

Unfortunately, fraud proceedings in criminal matters are painfully slow in Luxembourg and, since the victim barely has access to the case file, they are not very attractive; the result of which being that practitioners mostly turn away from criminal proceedings unless there really is no other option.

2 Foreign requests for mutual judicial assistance in criminal matters

Foreign requests for mutual assistance in criminal matters are usually executed in a timely manner by Luxembourg authorities. The judicial remedies against mutual assistance available in Luxembourg have become, over time and through a number of modifications of legislation, very limited, in that the suspect is generally not informed of the existence of such request and its execution by the authorities, and the bank does not have the right to inform a suspect of the freezing of his account.

The general concept of this legislation, based on Luxembourg's strong intent to fulfil its international obligations, is that any judicial remedies against such foreign request should be undertaken in the country making the request, and not in Luxembourg.

Bona fide third parties to the investigation have the right to be informed of the existence of the request and have a judicial remedy available in order to protect their rights.

Any evidence collected under such request for judicial assistance in criminal matters may only be used, by the requesting State, in the proceedings for which the request has been made, but not in other types of proceedings.

The judicial assistance will not be granted if it relates to offences, which are qualified as "political" under Luxembourg law, or if it relates exclusively to offences against tax laws or foreign exchange rules or if the request violates essential interests of the country or is a risk to its sovereignty or national security.

However, the actual verification on this is virtually non-existent, as the means of control by Luxembourg jurisdictions are limited and the legal remedies non-existent.

3 Confiscation

In national criminal proceedings, confiscation may be ordered over assets of any kind, including any revenue of these assets, as well as over assets which have substituted the assets mentioned before.

Any assets belonging to *bona fide* third parties

will not be subject to confiscation but will be returned to them.

As far as foreign confiscation decisions are concerned, they may be enforced in Luxembourg after having obtained an exequatur, which is awarded by way of national two-instance proceedings where the convict is heard. The exequatur may be refused for a number of reasons, such as, for example, political offences, or in case of a violation of the European Human Rights Convention, etc.

Third parties may claim their rights in the Luxembourg exequatur provisions, unless they had the possibility to already claim their rights during the foreign proceedings, but they did not do so.

4 Anti-money laundering framework

Luxembourg has one of the toughest anti-money laundering frameworks in place, and violations by professionals subject to AML rules are punished rather severely and with a lot of publicity.

5 Unexplained wealth orders

A recent law has introduced the concept of unexplained wealth orders into Luxembourg law.

They have quite a broad area of application and give the State Prosecutor substantial powers, but have not been tested much in case-law so far.

B Framework for civil remedies

1 Jurisdiction

The EU rules are applicable as far as jurisdiction is concerned. Luxembourg is also a party to a number of international conventions relating to jurisdiction, such as the Lugano Convention.

In cases where neither an international convention nor EU rules are applicable, Luxembourg Courts generally have jurisdiction if the defendant resides in Luxembourg. Also, if a case is initiated by a Luxembourg resident against a foreign national who is not resident in the EU or a country with which Luxembourg has concluded an international convention, Luxembourg Courts will accept jurisdiction.

The Luxembourg Courts generally also accept jurisdiction clauses, even if agreed upon by two parties, which do not have any connection with Luxembourg.

The simple fact that part of the assets relevant to a Court case are located in Luxembourg will generally not be sufficient for Luxembourg Courts to take jurisdiction over the entire case, unless the assets are immoveable property such as real estate. This principle does not, however, apply to conservatory measures for which Luxembourg Courts will accept jurisdiction.

2 Court proceedings

Legal proceedings are generally initiated by a summons to appear (an *assignation,* which is a deed served by a bailiff, the *huissier*), which needs to fulfil some formal requirements to be valid. Further, it needs to contain a detailed description of the facts and of the exact relief sought; otherwise, it will be voided by the Courts for *obscuri libelli.*

Civil proceedings may either be of pure civil nature or of commercial nature.

Pure civil proceedings are in writing, meaning that the parties' lawyers exchange written submissions between them and, when the preliminary written phase is concluded, the Court will hear the parties during a short hearing, in which the Court may require further explanations. The cases are usually not pleaded again orally during these hearings (a full pleading is highly unusual), but certain points may be clarified. It is therefore usual for the parties to simply refer to their written submissions during such hearings. This makes these proceedings quite slow and burdensome.

In commercial proceedings (e.g. proceedings between two merchants (*commerçant*) or between commercial companies, or proceedings brought by an individual against a merchant or a commercial company), first instance proceedings are subject to hearings where the parties present their oral arguments and the Court then renders a judgment, but the parties may also choose to conduct the proceedings in writing, in which case the procedure will be the same as for pure civil proceedings.

In appeal and in cassation, the proceedings will be only in writing.

Summary proceedings may be initiated by a claimant to seek interim relief, such as for the victim of a fraud to obtain a provisional allowance (if there are no contestations deemed to be serious), for a shareholder to suspend the effects of a general meeting of shareholders, to have a provisional administrator appointed for a company, a request for the appointment of a receiver over some assets (*séquestre*), to have an expert appointed to make technical findings, etc. Summary proceedings are usually reserved for urgent matters, but may still take some weeks if not months before a judgment is reached.

There are very limited possibilities to obtain *ex parte* orders, in case of serious urgency, but judges are quite reluctant to award such orders. Such *ex parte* orders may then be challenged in open court; the refusal to grant will also be challenged.

3 Conservatory measures

Luxembourg Courts accept to take jurisdiction for conservatory measures if the assets are located in Luxembourg (i.e. physical assets, claims, or assets held on a bank account, such as cash or shares or any other type of asset held, in any form, of financial institution).

Conservatory measures may be undertaken under Luxembourg law by way of a *saisie-conservatoire*, a *saisie-arrêt*, or a *saisie sur salaire*.

A *saisie conservatoire* allows a claimant to seize the assets of his debtors on a provisional basis. It will only be granted where there is urgency and a debt which is due and payable. The *saisie conservatoire* is authorised by the President of the District Court upon *ex parte* application. The asset which has been seized by way of a *saisie conservatoire* may not be sold (and the claimant paid) until the claimant has obtained an enforceable judgment against his debtor and validated the *saisie conservatoire*. It is to be noted that in practice the *saisie conservatoire* is rarely used.

The *saisie-arrêt* is used far more often. It allows a creditor to seize assets of his debtor which are in the hands of a third party such as, for example, the debtor's bank account, or a debt owed by a third party to the debtor.

The *saisie-arrêt* is either made on the basis of an enforceable title (such as a final judgment or an authentic title), or upon authorisation by the President of the District Court, if the claimant has no enforceable title, but has a claim which is certain, liquidated and payable. Such authorisation may be requested *ex parte* and an order authorising the *saisie-arrêt* is delivered upon such application, if the conditions are fulfilled.

In both cases, the deed of *saisie-arrêt* will be served by way of a bailiff first to the third party having a debt against the debtor and then to the debtor.

From the moment of the service of the deed of *saisie-arrêt*, the third party will have to block payment of all amounts it owes to the seized debtor (i.e. in case of a bank account, the whole account will be frozen even if there are assets on the account in excess of the debt).

In case of a *saisie-arrêt* authorised by the President of the District Court only, after the *saisie-arrêt* has been served upon the debtor, and until the Court is seized regarding the merits of the *saisie-arrêt*, the debtor may, by way of summary proceedings, request from the President of the District Court to have the order authorising the *saisie-arrêt* reviewed *inter partes* and to have it retracted or to have the effects of the *saisie-arrêt* limited to the amount of the claim for which the *saisie-arrêt* has been effected (a *cantonnement*).

In order to obtain the transfer of the claim which has been seized (and request payment thereof), the creditor has to request validation of the *saisie-arrêt* before the Luxembourg Courts. If

the Luxembourg Courts have jurisdiction over the case on the merits, they will hand down a judgment on the merits and on the validation of the *saisie-arrêt*.

If the Luxembourg Courts do not have jurisdiction on the merits, they will allow the claimant time to seek a judgment from a foreign Court and to have it declared enforceable in Luxembourg.

It is only after the judgment validating the *saisie-arrêt* has become final that the claim in the hands of the third party will be transferred to the claimant (who may then seek payment from the third party); and that the claimant may seek the third party to disclose which funds or assets are held on behalf of the debtor. This is done by way of a summons addressed by the creditor to the third party, the *assignation en déclaration affirmative*. This summons will also, if the above conditions are fulfilled, lift bank secrecy. If the claimant has an enforceable title, the *assignation en déclaration affirmative* may however be served on the third party before the *saisie-arrêt* is validated.

Until this *assignation en déclaration affirmative* has been served, the creditor will not know whether his *saisie-arrêt* has been efficient, i.e. whether any assets have been frozen, especially where bank accounts are frozen, given bank secrecy, which is only lifted after this summons.

This entails that it only makes sense for a creditor to undertake a *saisie-arrêt* in the hands of a third party where the creditor is sure that there are assets. If the creditor does not know at which bank his creditor has an account, and whether there is any money on such account, the creditor could theoretically serve a deed of *saisie-arrêt* on a number of different banks, but the costs of such proceeding do rapidly become elevated thus rendering it unfeasible in practice.

A *saisie sur salaire* allows the claimant to seize a debtor's salary in the hands of the employer, where the claimant has a certain, liquidated and payable claim. Once the *saisie sur salaire* is validated, the debtor's employer will directly pay part of the salary (a minimum of the salary is protected against the *saisie* to allow the debtor to buy food and pay for his rent) to the creditor instead of the debtor.

4 Pre-trial discovery

Luxembourg law does not provide for a pre-trial discovery regime as one would know from the United States, but there is the possibility to obtain pre-trial communication of certain documents, in accordance with article 350 of the New Code of Civil Procedure, according to which a claimant, under certain very specific conditions, may seek to obtain documents from the defendant in a fraud case or any other third party. The conditions are as follows:

- the result of the case on the merits has to depend on the fact for which the conservation or the establishing of the evidence is requested;
- the motive for obtaining such evidence has to be legitimate;
- the requested measures have to be legally admissible;
- the request has to be made before any Court case on the merits is initiated (otherwise the request will be refused); and
- the claimant has to describe in detail what evidence is sought, he may not simply limit himself to requesting the production of all evidence related to a potential Court case.

The seeking of evidence for the mere purpose of appreciating the opportunity of initiating a Court case on the merits will not be sufficient for the disclosure order to be granted.

Such a disclosure request is initiated by way of summary proceedings held in front of the President of the District Court.

5 Register of beneficial owners

In 2019, Luxembourg introduced a register of beneficial owners, whereby a company has to disclose the name and address of any person having a beneficial interest higher than 25% in the company.

An important number of companies have still not filed the relevant information with the register, but most entities that are domiciled with a registered agent have.

The weakness of this register is that a number of companies have circumvented the rules by issuing bonds convertible into shares, and thus hiding the true beneficial owner as a creditor, and thereby avoiding publicising the information about them.

In our view this is a fraudulent manoeuvre, but it remains to be tested in court.

All in all, this register is a very small progress towards easier fraud investigations, even though its practical use still remains to be tested.

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

Most fraud cases we deal with only have a partial Luxembourg element to them, which means that in these types of cases Luxembourg counsel only intervenes in a small part of the case, mostly to freeze assets or enforce a judgment against assets located in Luxembourg, or to find out information about assets held by a Luxembourg entity.

However, in our work as insolvency receivers, we regularly conduct fraud investigations ourselves.

Whatever the type of case, typically, what we would do first would be to check the documentation which is available at the Trade and Companies Register in relation to any entity involved in the fraud scheme, as well as the register of beneficial owners for these entities.

For the moment, the register of beneficial owners does not allow to retrieve the entities in which a person has an interest on the basis of that person's name, but it could be contemplated to try to obtain an injunction against the register, forcing the latter to run a search against the person in their register.

We would also run a verification on whether any of the persons and/or entities involved own any real estate in Luxembourg, even though access to this type of information has been rendered considerably more difficult with the arrival of GDPR. It is also possible to verify, on the basis of a Court order, whether a person is employed in Luxembourg or is paid a pension by the Luxembourg State.

At this stage, if there are the slightest thoughts that the perpetrators may have bank accounts in Luxembourg, we would seek a freezing order (*saisie-arrêt*) as described above.

If there is a very strong urgency in the case and a severe risk of disappearance of the funds, the best options would be to contact Luxembourg's Financial Intelligence Unit, with the goal of obtaining a provisional blockage of the funds held in Luxembourg to avoid any spoliation thereof, and then request civil conservatory measures on top.

Generally, any measure that we would seek would first be sought *ex parte*, and only upon refusal of an *ex parte* application, *inter partes*.

We would also contemplate using insolvency of a Luxembourg entity as a tool to recover assets or engage the liability of company officers (*de jure* or *de facto* ones). To that regard we should mention that Luxembourg Commercial Courts have, so far at least, been pretty open to litigation funding in relation to insolvency proceedings, even though, in general, litigation funding is not yet fully established in Luxembourg.

Parallel proceedings: a combined civil and criminal approach

In Luxembourg, the introduction of criminal proceedings is generally only useful where the victim (or the civil complainant) has not gathered enough evidence to support a civil claim on its own and needs the help of the coercive tools of criminal law to obtain such evidence.

Criminal proceedings, especially in complex fraud cases, are usually slower than civil proceedings and the victim loses control of the proceedings, which lie entirely in the hands of the public authorities. The victim could introduce criminal proceedings directly before the Criminal Courts by way of a direct summons (*citation directe*), but there is no direct advantage of proceeding that way as the risks of a trial of criminal nature are not avoided (at civil level, the proof of the wrongdoing is much easier as the criteria are lower: the simplest wrongdoing (*culpa levissima*) will generally trigger civil liability).

Also, Luxembourg investigating authorities are very reluctant to use mutual legal assistance tools, for reasons that are, to be honest, not entirely clear today.

The biggest issue is, however, that criminal proceedings will automatically entail a stay on any civil proceedings related to the same facts.

Therefore, it makes only little sense to initiate criminal proceedings unless there is absolutely no other choice, as these would block the whole civil recovery for a long period of time.

In our practice, we almost totally refrain from filing criminal proceedings and put weight only on civil remedies, which can be useful enough.

Key challenges

1 Bank secrecy laws

One of the essential concepts of the Luxembourg financial sector is the professional secrecy obligation, which is applicable not only to banks but also to the professionals of the financial sector (PSF), and is, in essence, an obligation to keep all the information obtained by a bank or PSF relating to its client confidential.

The breach of this duty of confidentiality constitutes a criminal offence sanctioned by imprisonment from eight days to six months and a fine of €500 to €5,000.

The duty of confidentiality is provided for by article 41 of the law of 5 April 1993 on the financial sector, which imposes a duty of confidentiality on the professionals of the financial sector (including banks), their employees, managers, directors and even their liquidators.

This article also provides that the wilful violation of the professional secrecy obligation constitutes the offence of breach of professional secrecy incriminated by article 458 of the Luxembourg criminal code, which essentially determines the duty of confidentiality of doctors, pharmacists and lawyers.

As a result, the duty of confidentiality of professionals of the financial sector is of the same substance as that of the latter professions.

The duty of confidentiality can only be overridden in very limited circumstances, such as:

- where there is a statutory provision (even prior to the law of 5 April 1993) authorising the revealing of confidential information;
- *vis-à-vis* national or international authorities in charge of prudential supervision if they are acting within their legal framework, and only if they are also bound by a duty of confidentiality;
- where the professional of the financial sector has to defend his interest in a Court case for his own cause;
- where a professional of the financial sector is called as a witness by a Court;
- *vis-à-vis* criminal authorities (such as an Investigating Magistrate who may require the professional of the financial sector to provide evidence on movements or owner of bank accounts concerned by an investigation);
- in case of money laundering: professionals of the financial sector are compelled, by law, to make a suspicious transaction report to the Public Prosecutor if they suspect money laundering; and
- in case of a *saisie-arrêt* that has been validated, the professional of the financial sector is obliged to disclose the information on his client against whom the *saisie-arrêt* has been validated.

However, the client's authorisation does not allow the professional to disclose confidential information subject to its duty of confidentiality.

Finally, Luxembourg has started to sign a number of bilateral non-double taxation treaties with other countries based on the OECD model convention and which contain provisions on automatic exchange of information in tax matters. A law was also introduced in 2012 authorising the Luxembourg tax authorities to collect information from the entities holding them (including banks). Basically, this means that the duty of confidentiality may be lifted in tax matters, if the originating Member State concluded a non-double taxation treaty with Luxembourg based on the above model treaty.

2 Securitisation vehicles

In my recent experience, the biggest challenge we face in Luxembourg are securitisation vehicles, which have now come up a number of times in fraud cases.

As per Luxembourg law, securitisation vehicles are quite opaque and are only subject to outside regulation if they offer their shares to the public, which is rarely the case. Also, an investor into a securitisation vehicle is not allowed to petition for insolvency of the vehicle, and some vehicles even cut off any rights of the investors to seek a judgment against such vehicle, which opens the door to fraud.

We have seen the case where such vehicles are set up and functioning as a form of investment fund. Even if these unregulated securitisation vehicles are often reserved for qualified investors, there are no real control mechanisms in place, which can result in shares ending up in the wrong hands.

This is, in our view, a result of the legislation for securitisation vehicles being too lax and definitely in need of being verified and/or secured for investors, as the fraud cases in relation to these vehicles keep on piling up.

Cross-jurisdictional mechanisms: issues and solutions in recent times

Mutual legal assistance in criminal matters has become much more effective recently, as Luxembourg law has eliminated all forms of appeal, with the result that nowadays mutual

assistance is granted almost automatically, with very little review by the courts as to whether the conditions are fulfilled.

Technological advancements and their influence on fraud, asset tracing and recovery

While Luxembourg brands itself as a favourable environment for startups (and we do have a substantial number of Fintech companies), when it comes to the combat of fraud, Luxembourg unfortunately lags a bit behind, especially at the level of the authorities, where there is some room for technological progress.

At the level of the private sector, one can certainly feel an important evolution in the use of technology; however, things are rendered a tad complicated by Luxembourg's multilingual environment: the day-to-day language is Luxembourgish, which is technology-resistant, while the official languages are German and French. Add to that, that English is used regularly in business, as well as the fact that Luxembourg has substantial expat communities from other countries that speak other languages than the four above, you have the right recipe for making it very difficult to use any technology that is not language-neutral.

Recent developments and other impacting factors

The most important recent development certainly is the register of beneficial owners.

As described above, it allows for any person to look up the beneficial owner of a Luxembourg company, even anonymously. Luxembourg has moved to full transparency as you can see.

There is, however, a number of caveats to this.

So far it is not possible to do a reverse search through the database of the register, i.e. to find companies that a specific person is the beneficial owner of.

It could, however, be contemplated to try and obtain an injunction against the register in order to force the latter to disclose the names of the companies that a person has a beneficial interest in.

To the best knowledge of the author, this has not been tried so far, but should definitely be an avenue to explore.

Max Mailliet specialises in litigation with a focus on fraud and asset tracing, white-collar crime, commercial and shareholder litigation and high-profile insolvencies.

Prior to opening his own firm, E2M, in 2008, Max was an associate in the litigation and corporate law departments of a major Luxembourg law firm. With his team, Max specialises in litigating complex fraud cases in front of the Luxembourg courts, including cases with an international element. Max and his team also regularly represent institutional clients in litigation related to financial matters, such as disputes between investment funds, between funds and their service providers, or between shareholders, in which Max has a very extensive experience.

Max is regularly appointed by the Luxembourg courts as insolvency receiver or liquidator in complex insolvency cases including multi-jurisdictional issues and asset recovery.

Max is also a lecturer in Luxembourg insolvency law. He is the Luxembourg exclusive representative to the ICC's FraudNet, a network of lawyers specialised in fraud and asset tracing.

Max studied at Robert Schuman University in Strasbourg and the London School of Economics and Political Science.

max.mailliet@e2m.lu

Singapore

Lee Bik Wei
Allen & Gledhill

Lee May Ling
Allen & Gledhill

Singapore has positioned itself as one of the leading centres, especially in Asia, for banking and financial services. A corollary to this is the increased risk of fraud, particularly with the growing prevalence of digital transactions. As such, it is unsurprising that Singapore has, over the years, made efforts to improve its regulatory framework and introduce harsher penalties for fraud-related offences. See, for example, the Serious Crimes and Counter-Terrorism (Miscellaneous Amendments) Act 2018, which increased the penalties under the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act for, *inter alia*, the failure to report suspicious transactions. This will be discussed in detail in the last section.

This chapter seeks to first outline the mechanisms through which victims of fraud may seek recourse, before going on to explore the reasons underlying the rising rates of fraud in Singapore. We consider both criminal and civil law in this chapter.

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

In Singapore, both civil and criminal actions (which give rise to different remedies) can be pursued against the perpetrator(s) of fraud. Civil proceedings are initiated by the victim, whereas criminal proceedings are generally initiated by the Attorney-General's Chambers (AGC) (save for in the limited case of private prosecutions). This section outlines the statutory framework and tools used in civil and criminal proceedings to pursue fraud claims.

Civil actions

The common causes of action commenced against perpetrator(s) of fraud in civil actions include:
(1) tort of deceit or fraudulent misrepresentation;
(2) breach of duty (fiduciary or otherwise);
(3) unjust enrichment; and
(4) tort of conversion.

Person(s) who have assisted the main perpetrator, or have received or helped transmit the proceeds of fraud, can also be joined as defendants in civil actions. The common causes of action relied upon here include:
(1) conspiracy;
(2) dishonest assistance; and
(3) knowing receipt.

In such proceedings, matters concerning evidence, identification and seizure of assets often arise. General tools which victims rely on include: (i) *Mareva* injunctions; (ii) *Anton Piller* orders; and (iii) Discovery orders. We explain these briefly below.

Mareva injunction

In civil claims involving allegations of fraud, it is common for a plaintiff to consider whether it might be possible to seize and secure assets or the proceeds of fraud via court proceedings. This is most commonly done by way of taking out an application for a *Mareva* injunction or freezing order. Such an application is usually taken out at the same time as commencement of the civil proceedings and on an *ex parte* basis, so as to ensure that the defendant does not have notice of the proceedings and does not have time to dissipate his assets. The reasons for taking out an *ex parte* application must be set out clearly in the supporting affidavit. Even so, in an *ex parte* application, the Singapore court rules require that the plaintiff/applicant notify the other party a minimum of two hours before the hearing, except in cases of extreme urgency or with the leave of Court.

The threshold to meet in order to obtain a *Mareva* injunction is high. There are also further considerations where one is seeking an extraterritorial injunction.

A court can grant a domestic *Mareva* injunction (i.e. over assets held in Singapore) where the following conditions are met:

(1) there is a valid cause of action over which the Court has jurisdiction, that the *Mareva* injunction is collateral to;
(2) there is a good arguable case on the merits of the plaintiff's claim;
(3) the defendant has assets within the court's jurisdiction. This includes all assets beneficially held by the defendant, but excludes assets which the defendant legally owns but holds on trust for third parties; and
(4) there is a real risk that the defendant will dissipate their assets to frustrate the enforcement of an anticipated judgment by the court.

It bears mentioning that even where fraud is alleged, this does not necessarily satisfy the last requirement that there is a real risk of dissipation. The Singapore courts have held that while a well-substantiated allegation of dishonesty will often be relevant in assessing the risk of dissipation, the court will still examine the nature of dishonesty alleged and the strength of evidence in support. As such, a good arguable case of dishonesty in itself was insufficient to show that there was a real risk of dissipation.

As for an extraterritorial *Mareva* injunction (i.e., over assets held outside of Singapore), broadly speaking, this can be granted by the court if the same conditions as a domestic *Mareva* injunction are present. However, the circumstances that will be required to show that an injunction is necessary will likely be more exacting in the case of a worldwide *Mareva* injunction. The plaintiff/applicant must show that the defendant has assets outside the court's jurisdiction. If the defendant has assets both within and outside the court's jurisdiction, it must then be shown that there are insufficient assets within the court's jurisdiction to satisfy the plaintiff's claim.

As part of the application for a *Mareva* injunction, the plaintiff will be required to provide an undertaking to comply with any order for damages (for loss sustained by the defendant and third parties as a result of the *Mareva* injunction) that the court may make (if any). To support this undertaking, the plaintiff may be required to:

(1) make a payment into court;
(2) provide a bond by an insurance company that has a place of business in Singapore;
(3) provide a written guarantee from a bank that has a place of business in Singapore; or
(4) make a payment to the plaintiff's solicitor that is to be held by the solicitor as an officer of the court pending any order for damages.

In an *ex parte* application for a *Mareva* injunction, the plaintiff is required to provide full and frank disclosure, in that the court must be fully informed by the plaintiff of all material facts. Where an application for a *Mareva* injunction does not contain all material facts, and this is brought to the attention of the court by, for example, the defendant, this may thwart the plaintiff's attempts to seize or secure the defendant's assets.

In principle, evidence of a collateral or ulterior purpose on the part of the plaintiff could justify the refusal of a *Mareva* injunction, although this would ordinarily be difficult to establish at an early stage of proceedings in which *Mareva* injunction applications are usually brought.

Anton Piller orders

In respect of obtaining evidence for the purpose of proving a claim of fraud, a plaintiff can apply to search premises and seize evidence by way of an *Anton Piller* or a search order. As with a *Mareva* injunction, this is usually done at the same time as commencement of the civil proceedings and on an *ex parte* basis, so as to ensure that the defendant does not have notice of the proceedings and does not have time to destroy evidence. Given the intrusive nature of an *Anton Piller* order, the threshold that must be met to obtain an *Anton Piller* order is naturally also a high one.

An *Anton Piller* order may, in general, be granted if the following conditions are met:

(1) there is an extremely strong *prima facie* case of a civil cause of action;
(2) the potential or actual damage to the plaintiff, which the plaintiff faces if the *Anton*

Piller order is not granted, is serious;

(3) there is clear evidence that the defendant has incriminating documents or items in their possession; and

(4) there is a real risk that the defendant may destroy the above documents or items before an application *inter partes*, i.e. where the application is served on the defendant and both sets of solicitors attend the application hearing, can be made.

However, even if the above conditions are met, a court may not necessarily grant an *Anton Piller* order. Rather, a court will only do so after determining that the prospective harm the plaintiff faces (as a result of the *Anton Piller* order not being granted) outweighs the prospective harm that the defendant faces (as a result of the order).

Similarly, as part of the application for an *Anton Piller* order, the plaintiff will have to undertake to pay damages sustained by the defendant as a result of the *Anton Piller* order if so ordered by the court. In addition, the plaintiff must also undertake to comply with an order for damages that the court makes in connection with a finding (if any) that the actual carrying out of the *Anton Piller* order was: (1) in breach of the terms of the order made; or (2) otherwise inconsistent with the plaintiff's solicitors' duties as officers of the court.

To support this undertaking, the plaintiff may be required to take actions similar to those in an application for a *Mareva* injunction, such as making a payment into court or providing a bond or guarantee. The plaintiff is also required to make full and frank disclosure in an application for an *Anton Piller* order.

Pre-action disclosure

Where evidence needed for a civil suit lies with a third party (rather than the defendant), pre-action disclosure may be necessary. Pre-action disclosure can take place in various forms: third-party discovery; third-party interrogatories; or a *Bankers Trust* order, i.e. disclosure orders made against banks to disclose documents to assist with tracing claims, so termed after the eponymous *Bankers Trust Co v Shapira* [1980] 1 WLR 1274 case.

A prospective plaintiff may apply for a *Norwich Pharmacal* order, i.e. pre-action disclosure orders for the purpose of identifying potential defendant(s), so termed after *Norwich Pharmacal Co v Customs and Excise Commissioners* [1974] AC 133, which can either take the form of third-party discovery of documents or third-party interrogatories. In Singapore, the Court's jurisdiction to grant such orders is statutorily codified in Order 24, rule 6(5) and Order 26A, rule 1(5) of the Rules of Court, respectively. It is also noted that the Singapore High Court in *Success Elegant Trading Ltd v La Dolce Vita Fine Dining Co Ltd and others and another appeal* [2016] 4 SLR 1392 left open the question of whether the court has an "inherent jurisdiction" to grant pre-action disclosure outside of the provisions in the Rules of Court (at [56]).

The following conditions must be met:

(1) the third party had facilitated the wrongdoing, though such facilitation may be innocent;

(2) there is a reasonable *prima facie* case of wrongdoing by the unidentified perpetrator(s); and

(3) granting the order is necessary to enable the plaintiff to bring proceedings, or it is just and convenient in the interests of justice to grant the same.

Where the third party is a bank, an application can be made for a *Bankers Trust* order to assist the applicant in a potential tracing claim. The banking secrecy rules in the Banking Act would be overridden where the victim can demonstrate that there is a substantive right to disclosure, by virtue of s 175 of the Evidence Act, see also *Wee Soon Kim Anthony v UBS AG* [2003] 2 SLR(R) 91 at [20]. Generally, the applicant must show that the same conditions have been met as required for a *Norwich Pharmacal* order. However, it has been argued that a higher threshold should apply for a *Bankers Trust* order, requiring that the applicant show a *compelling* (rather than reasonable) *prima facie* case of fraud. This has not been decided upon by the Singapore courts (*Success Elegant Trading Ltd v La Dolce Vita Fine Dining Co Ltd and others and another appeal*).

Civil remedies

There are generally two types of remedies a victim may be awarded where fraud has occurred: personal remedies; and proprietary remedies. A personal remedy results in a debt owed personally by the defendant to the plaintiff. Where the assets of the defendant are insufficient to satisfy the claim, the plaintiff will rank equally with the defendant's other creditors. On the other hand, a proprietary remedy results in a claim to a specific property (or its traceable substitutes) which has passed to the defendant. Proprietary remedies are generally preferred by victims of fraud as this allows them to trace the property into the hands of downstream recipients, which is a common occurrence in fraud cases.

In *Standard Chartered Bank v Sin Chong Hua*

Electric & Trading Pte Ltd & Ors ([1991] 2 SLR(R) 445; [1991] SGHC 121), when the fraud was discovered by the plaintiff bank, the perpetrators had already dispersed the money into other accounts, including that of the second and fourth defendants. The court held that the plaintiff bank nevertheless retained an equitable proprietary interest entitling it to trace the proceeds into the defendants' bank accounts.

Whether a proprietary remedy is available will turn on the facts of the case and the cause(s) of action being pursued. The above section has previously highlighted the common causes of action pursued in Singapore in respect of fraud. Amongst these, proprietary remedies (usually a constructive trust) have been awarded for:

(a) breach of fiduciary duty;
(b) breach of trust;
(c) knowing receipt; and
(d) dishonest assistance.

Criminal actions

Where fraud has occurred, this may potentially constitute one (or more) of the various offences set out in the Penal Code (Cap 224, 2008 Rev Ed; see e.g., Sections 403, 405, 407, 409, 411, 415, 421-424A, 463, 468 and 477A), the Companies Act (Cap 50, 2006 Rev Ed) Sections 157, 401, 402 and 406 and the Income Tax Act (Cap 134, 2014 Rev Ed) Sections 96 and 96A. New Penal Code offences relating to fraud were first introduced in 2019 and came into effect on 1 January 2020. While there is little case law on these new provisions, it is expected that these provisions will make it easier to bring perpetrators of fraud to task. This will be discussed further below in Section 7.

There is no limitation or time bar in respect of criminal offences in Singapore. The police possess broad powers of investigation in Singapore under the Criminal Procedure Code, including powers of search and seizure, which they can use to investigate the alleged fraud (s 34, s 35 of the Criminal Procedure Code). Police possess automatic powers of search and seizure where the offence is one that is arrestable without warrant, and can also be granted search and seizure orders.

Corporate governance reforms

Outside of legal proceedings, statutory reforms in Singapore have also sought to reduce fraud by increasing independence and monitoring of corporate governance boards. The 2018 Code of Corporate Governance (Monetary Authority of Singapore, 6 August 2018) sets out certain threshold requirements for, *inter alia*, board composition. For instance, the 2018 Code requires a majority of the Board to be independent (Provision 2.2) where the Chairman is not independent – "independent" being defined as, *inter alia*, having no relationship with the company, its related corporations, its substantial shareholders or its officers that could interfere, or be reasonably perceived to interfere, with the exercise of the director's independent business judgment in the best interests of the company: 2.1 of the Code of Corporate Governance – reflecting a higher threshold than the 2012 Code, which only required half the Board to be independent in such a situation (Monetary Authority of Singapore, *Code of Corporate Governance*, 2 May 2012 at Guideline 2.2).

2 Case triage: Main stages of fraud, asset tracing and recovery cases

When fraud is first brought to the attention of the victim, which may be through avenues such as whistleblowing, the external authorities or internal audits, the victim will usually commence an investigative process to find out, *inter alia*, who perpetrated the fraud, when the fraud was carried out and where the monies have been dissipated to.

The victim may choose to file a police report at this stage. After the filing of a police report, the police will likely ask the victim to attend a police interview and take his statement. Investigations into fraud are usually conducted by the Commercial Affairs Department (CAD). The CAD has powers to, *inter alia*, seize property (including monies in bank accounts) under the Criminal Procedure Code. Following the conclusion of the investigation, the AGC, with the recommendation of the authority or agency investigating the purported offence, will decide whether to: (1) charge the perpetrator; (2) give the perpetrator a warning; or (3) take no further action. Should bank accounts be frozen pursuant to police investigations, the CAD may choose to return the recovered sums (if any) to the victims. The victim may also commence civil proceedings to attempt to recover the misappropriated sums. The victim may concurrently apply to court for injunctive relief in order to freeze the assets of the defendant and/or to obtain more information on the location of his assets. See above at Section I for more information on the available mechanisms.

After judgment has been obtained, there are various modes of enforcement available to the victim should the defendant fail to comply. Often, a successful claimant will apply for a garnishee order against the defendant's bank account, which compels the bank to pay the claimant out of the defendant's bank account. Another common manner of enforcement is to apply for a writ of execution in order to attach property of the defendant and effects its sale.

3 Parallel proceedings: A combined civil and criminal approach

Parallel proceedings for fraud occur fairly frequently in Singapore. This is because criminal proceedings do not give the victim any monetary compensation for the fraud (unless a compensation order is made by the court). In addition, as mentioned above, criminal proceedings are

independently spearheaded by the AGC and the victim does not have control over such proceedings.

There is no obligation on the police to reveal information obtained in the investigative process to the victim, even if such information would assist the victim's civil claim. For these reasons, victims of fraud of substantial amounts typically choose to also pursue civil action against the perpetrators to recover the losses suffered.

A victim may choose to file a magistrate's complaint with the State Courts of Singapore, particularly where authorities have declined to investigate or take action. A magistrate's complaint is generally filed by an individual wishing to commence private prosecution (as opposed to prosecution by the state). The AGC may still choose to take over the conduct of proceedings or discontinue the prosecution (Section 13 of the Penal Code).

4 Key challenges

Cyber fraud

Based on the statistics from the Singapore Police Force, commercial fraud in Singapore has become more prevalent (see for example: Singapore Police Force, *Mid-Year Crime Statistics for January to June*

2019, 30 August 2019). This is likely due in part to the increase in cyber fraud, for which it is difficult to track down foreign perpetrators. In response, a centralised unit within the CAD has been set up to tackle fraud, in particular e-commerce scams. This new unit collaborates with three major banks in Singapore, allowing bank accounts suspected of fraud to be frozen within days. In the past, fraudulent bank accounts could take up to two months to be frozen. The new system also allows for investigating officers to send out one centralised order requesting for information from all three banks, as opposed to three separate orders. Increasing the rate of response to fraud is crucial in view of the rapid rate at which online fraud is perpetuated.

5 Cross-jurisdictional mechanisms: Issues and solutions in recent times

Cross-jurisdictional issues may arise where the aid of Singapore courts is sought to trace assets in respect of fraud committed abroad. In the same vein, legal proceedings commenced locally may also require foreign assistance to trace assets dissipated overseas. It is apposite to highlight that tracing is not a claim nor remedy, but only a process which identifies an asset as substitute for the original asset that belongs to a claimant.

Tracing of assets in aid of foreign proceedings

Singapore's apex court has held that the Court's power to order pre-action disclosure under the Supreme Court of Judicature Act does not extend to pre-action disclosure in aid of proceedings beyond Singapore. Given that pre-action disclosure is often required for the purposes of tracing and following a victim's money, this may present foreign parties with further challenges in seeking to trace their misappropriated assets into Singapore.

Having said that, the courts have held that where there is sufficient nexus to Singapore, such pre-action disclosure may be granted. There will be a clear nexus to Singapore where, for instance, there is a likely prospect of subsequent proceedings being commenced in Singapore. It has also been argued that the court *may* have the inherent jurisdiction to order pre-action discovery in aid of foreign proceedings even if such power does not exist under the Rules of Court. However, this has not been decided.

As for *Mareva* injunctions, the current position is that the Singapore courts have the power to grant a *Mareva* injunction in aid of foreign proceedings under s 4(10) of the Civil Law Act where it is "*just or convenient*" if the following pre-requisites are met:

(1) the plaintiff has a reasonable accrued cause of action against the defendant that is recognised or justiciable, i.e., a claim for substantive relief which the court has jurisdiction to grant and a claim that can be tried by the court , in a Singapore court;
(2) the Singapore court has *in personam* jurisdiction over the defendants in respect of the Singapore action;
(3) there are assets within the territorial jurisdiction of Singapore which could be the subject of a *Mareva* injunction; and
(4) substantive proceedings are brought in Singapore against the defendant, although these proceedings might be stayed by the Singapore court in favour of proceedings elsewhere.

Complications may also arise where multiple jurisdictions are involved, making it challenging to determine which is the proper forum in which a claim should be heard. In international frauds where money is quickly transferred from one country to another, it may be especially challenging to identify the place of "ultimate enrichment" for the purposes of determining the applicable law ('*lex causae*').

In respect of criminal proceedings initiated abroad, overseas authorities can first

contact the Suspicious Transaction Reporting Office (STRO), which is Singapore's Financial Intelligence Unit. This will allow the STRO to liaise with its global counterparts and provide information to assist in the matter. For tracing assets, a request for mutual legal assistance (MLA) may be made to the International Affairs Division department of AGC. Under the Mutual Legal Assistance in Criminal Matters Act (MACMA), AGC will provide assistance in tracing in accordance with the provisions and requirements set out in MACMA.

Some specific tracing mechanisms that can be ordered in aid of foreign criminal proceedings are:

(1) taking of evidence before a Singapore magistrate for use in criminal proceedings pending in the court of a foreign country;
(2) production orders directed at financial institutions or persons if there are reasonable grounds for suspecting that the perpetrator has carried out or benefited from a foreign offence; and
(3) execution of searches and seizures to collect evidence, if there are reasonable grounds for believing that the thing is relevant to a criminal matter and is located in Singapore.

Enforcement of judgments granted abroad

Under the Reciprocal Enforcement of Commonwealth Judgments Act (Cap 264, 1985 Rev Ed.) (RECJA) and the Reciprocal Enforcement of Foreign Judgments Act (Cap 265, 2001 Rev Ed.) (REFJA), when certain requirements are met, judgments made by the superior courts of certain countries may be registered and enforced directly in Singapore. Currently, the REFJA and RECJA cover 11 jurisdictions; namely, the United Kingdom, Australia, Hong Kong, New Zealand, Sri Lanka, Malaysia, India (except the State of Jammu and Kashmir), Pakistan, Brunei Darussalam, Papua New Guinea and Windward Islands. It is generally easier to register a judgment pursuant to the REFJA than the RECJA due to the fact that registration under the former is available as a matter of right rather than as a matter of the court's discretion.

In respect of foreign judgments that do not fall within the RECJA and REFJA, these may generally be enforced under common law if the judgment is:

(1) for a definite sum of money;
(2) final and conclusive; and
(3) the foreign court has jurisdiction in the context of conflicts of law.

If a foreign judgment was obtained by fraud, the Singapore courts would be entitled to refuse enforcement of the judgment in Singapore under the RECJA, REFJA and common law.

6 Technological advancements and their influence on fraud, asset tracing and recovery

The anonymity of cryptocurrency transactions has made cryptocurrency a prime vehicle for fraud. Numerous advisories have been issued by Singapore's public authorities, including the Monetary Authority of Singapore (MAS) and the CAD in this regard.

In a bid to address these risks, the Singapore Parliament passed the Payment Services Act 2019, which introduces a regulatory framework for digital payment token services such as cryptocurrency exchanges. While this regulatory framework chiefly relates to money laundering and terrorism financing (as opposed to user protection), this nevertheless represents a significant step forward by subjecting cryptocurrencies to more stringent oversight. The new Act will also extend the scope of regulations (previously under the Payment Systems (Oversight) Act) by recognising various forms of e-money such as e-wallets (Payment Services Act 2019 (No. 2 of 2019) at section 2, defining "e-money"). The Payment Services Act will come into force on 28 January 2020.

Only one civil action has been heard in Singapore's courts involving bitcoin to date – *B2C2 Ltd v Quoine Pte Ltd* [2019] 4 SLR 17, albeit in the context of breach of contract and trust rather than fraud. As such, the impact of cryptocurrencies on asset tracing and fraud recovery still remains to be seen, given that these developments are still relatively nascent in Singapore.

More generally, technological advancements have meant that a vast amount of financial services and transactions are now conducted digitally, often via automated transactions. MAS has sought to address this by releasing Technology Risk Management Guidelines (Monetary Authority of Singapore, *Consultation Paper: Technology Risk Management Guidelines*, March 2019), which provide certain procedures that financial institutions must follow to reduce the risk of fraud. Such procedures include multi-factor authentication and end-to-end encryption (*id* at 14.2).

7 Recent developments and other impacting factors

Unlike other jurisdictions which may have legislation specific to fraud (see, for example,

the United Kingdom's Fraud Act 2006), offences involving fraud or dishonesty are currently statutorily encapsulated in various provisions in, *inter alia*, the Penal Code (see for example, s 411(1) of the Penal Code which criminalises receiving or retaining any property where there is knowledge that the property was obtained "through an offence involving fraud or dishonesty"), the Companies Act and the Income Tax Act. As of 6 May 2019, however, the Criminal Law Reform Bill introduced a new offence of fraud into the Penal Code which is adapted from the UK Fraud Act 2006 and an additional offence of obtaining services fraudulently (section 424A; see also the new offence of obtaining services fraudulently under section 420A). These provisions came into force on 1 January 2020.

These amendments will bring fraud legislation more in line with current world developments, as fraud today often involves highly complex and novel patterns. Under the previous regime, the provision of "cheating" required that there was a victim which relied on the deception. The new offence of fraud does away with the requirement that there be an identifiable victim, instead focusing on the intent of the offender. In complex online scams, it may be near impossible to illustrate "reliance" by the victim. This enactment was motivated in part by the LIBOR-fixing scandal, which Parliament recognised as one instance in which it would have been "*very difficult to show that the victims relied upon the fraudulent representations of the bank employees who manipulated LIBOR*" (*Singapore Parliamentary Debates, Official Report* (6 May 2019) vol 94 at 3.55pm).

The amendments also clarify the scope of jurisdiction that courts possess over offences committed abroad. A new Schedule has been added to the Penal Code, for which the court will have jurisdiction if the requirements under the new section 4B are met. Under section 4B, the court will have jurisdiction over the offence where any physical element of the offence occurs in Singapore or where a fault element of the offence involves an intention to make a gain or cause a loss or exposure to a risk of loss or to cause harm to any person in body, mind, reputation or property, and that gain, loss or harm occurs in Singapore. Specified offences under the Schedule include dishonest misappropriation of property, receiving stolen property and cheating. In other words, even where fraud is perpetrated overseas, the court may still possess jurisdiction so long as the harm occurs in Singapore. These amendments were specifically made with targeting multi-jurisdictional fraud in mind.

Further, the CDSA was amended in 2018 to increase the various penalties for money laundering, failure to report suspicious transactions and tipping off (Serious Crimes and Counter-Terrorism (Miscellaneous Amendments) Act 2018 (No. 51 of 2018)). A new offence has also been added to criminalise the possession of any property reasonably suspected of being or representing any benefit of criminal conduct. These provisions came into force in 2019.

Lee Bik Wei is the deputy head of the firm's white collar & investigations practice. She regularly advises clients on white-collar, regulatory and compliance and corporate governance matters, and regulatory and corporate investigations. These include matters involving criminal breach of trust, corruption, market misconduct, mutual legal assistance matters, and employee misconduct, fraud, and corporate governance-related issues.

Her main areas of practice also encompass commercial litigation and international arbitration. She has substantial experience in a range of areas including cross-border joint venture disputes, corporate disputes such as shareholder and/or directors' disputes, property and trust, and contentious employment disputes.

Bik Wei's clients include local companies and multinational corporations, both private and listed, and trust companies. Bik Wei is also proficient in Mandarin and has advised Chinese clients in arbitral proceedings.

lee.bikwei@allenandgledhill.com

Lee May Ling has an established background in general and commercial litigation. She has acted in a broad spectrum of cases, including employment disputes, misconduct and fraud cases, company and shareholder disputes, estate disputes and corporate-governance matters.

Her practice focuses on white-collar crime and investigations. She has developed particular expertise in advising multinational conglomerates, as well as small and medium-sized enterprises, in this sphere. This includes assisting them with navigating anti-fraud, corruption and money-laundering laws, conducting internal investigations into misconduct, fraud and harassment, as well as advising companies on dealing with authorities on regulatory issues, police investigations, and dawn raids.

May Ling graduated with first class honours from King's College London and also has an LL.M. in Commercial Law.

lee.mayling@allenandgledhill.com

Allen & Gledhill is an award-winning full-service South-east Asian law firm providing legal services to a wide range of premier clients, including local and multinational corporations and financial institutions. The firm is consistently ranked as a market leader in Singapore and South-east Asia, having been involved in a number of challenging, complex and significant deals, many of which are first of its kind. The firm's reputation for high-quality advice is regularly affirmed by the strong rankings in leading publications, and by the various awards and accolades. With a growing network of associate firms and offices, it is well-placed to advise clients on their business interests in Singapore and beyond, on matters involving South-east Asia and the Asian region. With offices in Singapore and Myanmar, its associate firm, Rahmat Lim & Partners in Malaysia, and its alliance firm, Soemadipradja & Taher in Indonesia, Allen & Gledhill's network has over 550 lawyers in the region.

www.allenandgledhill.com

ALLEN & GLEDHILL

Switzerland

Paul Gully-Hart
Schellenberg Wittmer

George Ayoub
Schellenberg Wittmer

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

1.1 General background

The Swiss legal system is based on a civil law tradition. Its principal sources for authoritative legal propositions are, respectively and by order of importance, written codes, judicial decisions and writings of legal scholars. In this respect, it is important to understand that the common law rule of a binding precedent is not recognised in Switzerland. However, considerable weight should be given to a line of judicial decisions establishing a particular legal proposition.

In 2011, the Swiss legal system experienced one of its most important developments. Both civil and criminal procedural provisions were unified and the 26 Swiss Cantons abandoned their own Civil and Criminal Procedure Codes in favour of the Federal Civil Procedure Code (CivPC) and the Federal Criminal Procedure Code (CrimPC).

Despite the unification of procedural rules, the organisation of the judiciary remains mainly in the hands of the Cantons. Federal law mandates Cantons to provide, subject to a few exceptions, for a two-instance judiciary system (first instance court and court of appeal) but grants the Cantons the powers to establish specialised commercial courts. Only four Cantons (Zurich, Bern, St-Gallen and Aargau) have established such courts which serve as a court of first and sole instance for commercial disputes. Other specialised courts, such as Labour Courts or Landlord and Tenant Law Courts, are by contrast more common.

The composition of courts is also regulated by the Cantons. Usually, a single judge is appointed at the first instance and a panel of several judges adjudicates disputes brought to the court of appeal. For specific matters such as labour, landlord and tenant disputes, the Cantons usually provide a panel composed of one professional judge and at least two layman judges who have professional experience in the field of disputes. This particular composition aims to ensure that the necessary practical know-how is available for resolution of disputes in specific fields of law.

However, there is no room in Switzerland for a jury system which was effectively abolished when the CrimPC came into force in 2011.

Issues relating to fraud, asset tracing and recovery may be adjudicated in civil litigation, i.e. in civil courts or specialised commercial courts in the Cantons where such courts have

been established (hereafter: section 1.2) or in criminal proceedings which may be conducted at a cantonal level or at a federal level (hereafter: section 1.3).

1.2 Civil litigation

It is important to understand that civil litigants may rely on the well-established doctrine of civil tort which provides for appropriate judicial relief and remedies in cases where a civil plaintiff is complaining of an unlawful action of a defendant that has caused the damage in respect of which recovery or compensation is being sought.

Civil proceedings in Switzerland can be summarised in three stages: (1) the assertion stage consisting in the presentation of facts by the parties to the court; (2) the evidentiary stage, which is mainly focused on taking evidence on relevant facts; and (3) the post-hearing stage where each party comments on the evidence provided to the court.

The first stage is initiated by the claimant filing a detailed written statement of claim with the court. In certain circumstances, a conciliation process before a court is mandatory. There is no general pre-trial disclosure rule and the parties determine all the facts and relevant evidence to be submitted to the court in their briefs. A claimant in Switzerland is expected to lay all his cards on the table at the beginning of the proceedings. Likewise, the defendant will also be given an opportunity to submit the facts that he deems relevant and to offer evidence proving those facts or rebutting the facts put forward by the claimant.

Swiss civil proceedings also provide mechanisms for the defendant to "pass on" liability by bringing an action against a third party by means of a "notice of litigation". That person will then become a party in the proceedings and therefore bear, together with the defendant, any losses and damages recognised by the court. Similar mechanisms are provided for in a joinder which is admissible if two or more claims raise a common question of fact or of law, and if the same proceedings apply to them.

Furthermore, a third party may join ongoing proceedings if it can show a credible legal interest in having a pending dispute decided in favour of one of the parties.

The second stage is where the evidence is taken. The general rule is that each party carries the burden of proving the facts upon which its claim or defence is based. Parties must present all available evidence in their initial submission. The court has a wide discretion in weighing up the evidence. In this regard, the court will designate the admissible evidence through a procedural order and will also determine which party carries the burden of proof and counter-proof.

There is no cross-examination of experts and witnesses as such, but parties may comment on the questions asked by the court and may put additional questions. Expert opinions commissioned by one of the parties and affidavits are not considered as admissible evidence as such under the CivPC, although in practice the court will assess them freely and they are generally only given the weight of party pleadings.

Unlike civil litigation conducted in a common law jurisdiction, it is generally not permissible to contact potential witnesses and to prepare them for litigation. Persons who are called upon to testify in civil proceedings are required to cooperate in the taking of evidence except where this would expose them to criminal prosecution or civil liability or where they are bound by a statutory obligation of confidentiality (mainly lawyers and doctors).

There is no contempt of court as such. However, the court may draw unfavourable inferences in case of lack of cooperation.

Finally, in the third phase, the parties have the opportunity to comment on the evidence that has been taken before the court hands down a judgment. Courts may not adjudicate more or something other than what the claimant has explicitly requested.

The court will determine the costs of the proceedings in the final judgment. The unsuccessful party usually bears all costs including court fees and a reasonable amount for the legal costs of the prevailing party. It is noteworthy that punitive damages are unknown in Swiss law.

Swiss law also provides for interim and injunctive relief in aid of civil litigation or to facilitate the enforcement of a future judgment in favour of the claimant. The most common remedy available is the so-called attachment order which is subject to three main requirements: (1) the petitioner has a *prima facie* claim against the defendant which has a reasonable chance of succeeding on its merits; (2) the assets to be attached are located in Switzerland; and (3) the petitioner relies on a valid ground for an attachment. The most common ground for an attachment is the absence of a domicile of the defendant in Switzerland or the absence of a registered office in Switzerland if the defendant is a legal entity.

However, if the petitioner relies on that ground, he must show that there is a sufficient nexus between the claim and Switzerland unless he is in a position to rely on a judgment in his favour or on a recognition by the defendant that the debt is owed. The requirement of a nexus in

Switzerland is usually fulfilled where one of the parties has its domicile in Switzerland, the place of execution or of performance of the contract is in Switzerland or where the unlawful action (tort) took place in Switzerland or where the harmful result of that action occurred in Switzerland.

Unlike a common law freezing order, a Swiss attachment order is an *in rem* remedy which only captures specific items of property which have been identified by the petitioner and which are located in Switzerland. It is also possible to attach claims of the debtor against a third party, provided that the third party is domiciled (or has its registered office) in Switzerland.

1.3 Criminal proceedings

Common law jurisdictions such as the UK provide civil claimants with an impressive toolbox of remedies available to them in cases involving fraud and the recovery of assets: worldwide freezing orders; extensive disclosure obligations; Norwich Pharmacal or Bankers Trust Orders; Search Orders under the supervision of an independent solicitor, etc.

Although most of these remedies are not available in civil litigation conducted in Switzerland, it is often possible for victims of fraud and other financial misconduct to assert their claims in the course of criminal proceedings.

This is particularly true in Switzerland: claims arising from economic crime may be asserted and adjudicated under Swiss criminal law to assist the claimants/victims in their efforts to recover assets.

The CrimCP has created and carefully defined two important notions: the notion of *"injured party"* also referred to as the *"person suffering harm"*; and the notion of a private claimant acting within the criminal proceedings (the *"plaintiff"*).

The Swiss Federal Tribunal (i.e. the Supreme Court of Switzerland) has held that the injured party within the meaning of Art. 115 § 1 CrimCP is the person who is entitled to the legally protected interest or right which is directly affected by the offence committed. It is enough that the legally protected interests are being threated.

A person entitled to file a criminal complaint is deemed in every case to be an injured party.

The plaintiff is an injured party who has expressly declared that he or she wishes to participate in the criminal proceedings as a criminal or civil claimant.

The status of a plaintiff therefore implies above all that the person qualifies as an injured party within the meaning of Art. 115 CrimCP.

However, while the status of an injured is acquired *ex lege*, the status of a plaintiff may result only from a choice that has to be made explicitly with an indication as to whether the plaintiff intends to act, cumulatively or alternatively, as a criminal or civil claimant.

It is perfectly conceivable for a person to participate in the criminal proceedings only to support the prosecution and not to make any civil claim. It is also conceivable for the plaintiff to, initially, limit his or her participation to one of the two aspects (criminal or civil) and to extend it to the other at a later point in time.

Under Art. 104 § 1 let. b CrimCP, the plaintiff is formally a party to the proceedings together with the accused person and, at the stage of the trial, the public prosecutor.

The plaintiff enjoys all the rights that the CrimCP provides to a party, such as the right to be heard (Art. 107 CrimCP), the right to submit requests and petitions to the public prosecutor (Art. 109 *et. seq.* CrimCP), to be assisted by a legal counsel to defend his or her interests (Art. 127 CrimCP), to attend the taking of evidence and to ask questions during hearings (Art. 147 CrimCP), to make parties admissions (Art. 346 CrimCP), to appeal decisions and actions that affect the legally protected interests of the plaintiff (Art. 382 CrimCP), and the right to seek compensation for the costs of the proceedings (Art. 432 CrimCP).

In addition to the above, the plaintiff may bring civil claims based on the offence as a private claimant in the criminal proceedings (Art. 122 to 126 CrimCP). This allows for the same judge to rule (1) on the guilt and sentence of the offender, and (2) on civil claims for damages.

Specific rules apply to civil claims brought in the context of criminal proceedings.

Art. 122 § 1 CrimCP provides that the injured party *"may bring civil claims based on the offence as a private claimant in the criminal proceedings"*.

The civil proceedings are pending as soon as a declaration to that effect is made by the plaintiff. In other words, the mere assertion of a claim by a plaintiff is sufficient to create *lis pendens*, regardless of the description of the claim and the statement of grounds which must be made, at the latest, at the trial during the pleadings (Art. 123 § 2 CrimCP).

The jurisdiction of the criminal court is thus determined solely by the fact that it has jurisdiction over the criminal case and the court hearing the criminal case will rule on the civil claims regardless of the amount involved.

Thus, the court handling the criminal case is called upon to adjudicate on all the civil claims that the plaintiff is entitled to raise against the defendants arising from the facts underlying the criminal conduct.

Prayers for relief are those that are based on civil law and which are ordinarily brought before the civil courts.

There are instances, however, where they may refer the matter to a civil court, e.g.:

- the criminal proceedings are abandoned or concluded by means of a summary penalty order;
- the claimant has failed to justify or quantify the claim sufficiently;
- the claimant has failed to lodge a security in respect of the claim;
- the accused has been acquitted but the court is not in a position to make a decision on the civil claim; or
- the public prosecutor in charge of the investigation has ordered the abandonment of the criminal proceedings.

If a full assessment of the civil claim will cause disproportionate work, the criminal court may make a decision on the merits of the claim and refer the plaintiff to a civil court or quantify the claim.

Thus, the law seeks to promote the full treatment of civil claims, validly brought by the plaintiff in the context of criminal proceedings.

In addition to the adjudication of civil claims, Swiss criminal law also provides for a remedy of restitution under Art. 70 of the Swiss Criminal Code (SCC) in situations where the proceeds of criminal conduct, at the expense of the individual rights of the plaintiff, have been confiscated. Art. 73 SCC further provides that the proceeds of crime may be allocated to the injured party, if its claims have been ascertained in court proceedings (which may be either civil or criminal).

1.4 Enforcement of foreign judgments

As a matter of Swiss law, no judgment or order granted by a foreign court may be enforced in Switzerland as long as it has not been recognised and declared enforceable by a Swiss court (exequatur proceedings).

The Federal Act on Private International Law (PILA; Art. 25-27) provides for the recognition and enforcement of foreign judgments, subject to certain formal and substantive requirements.

Switzerland is also bound by the Convention on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters of 30 October 2007 (the "2007 Lugano Convention").

Significantly, Art. 32 of the 2007 Lugano Convention provides that *"judgments mean any judgment given by a Court or Tribunal of a State bound by this Convention, whatever the judgment may be called, including a decree, order, decision or writ of execution, as well as the determination of costs or expenses by an officer of the court"*.

Interim orders such as worldwide freezing orders fall under Art. 32 of the 2007 Lugano Convention and can thus be recognised and enforced, subject to certain conditions.

The Swiss Federal Tribunal has adopted the same view regarding the recognition/enforcement of worldwide freezing orders, provided that the defendant has been given an opportunity to seek a discharge or variation of the order.

The only substantive requirement to obtain a declaration of enforceability of a foreign judgment or order under the 2007 Lugano Convention from a Swiss Court is that the decision is enforceable in the State of origin.

The formal requirements are set out under Art. 53 of the 2007 Lugano Convention:

- a copy of the judgment which satisfies the conditions necessary to establish its authenticity;
- a certificate issued by the Court or the competent authority where the judgment was given whereby the judgment is enforceable in the state of origin; and
- a certified translation of the documents mentioned above.

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

2.1 Preliminary steps

It is essential to have a full understanding of the relevant facts and to set out a legal strategy which will be driven by the facts and by the objectives assigned by the client.

If the dispute occurs in a multi-jurisdictional context (which is often the case), it will also be

necessary to reach out to the client's professional advisers in the other jurisdictions concerned to determine where the most effective legal action should be undertaken.

Legal strategy will also be influenced by the presence (or absence) of recoverable assets in the jurisdiction. For instance, if the debtor/defendant owns assets in Switzerland, priority may have to be given to interim/injunctive relief in Switzerland, such as an attachment order over the relevant assets eventually followed by legal action on the merits in the Swiss courts. Conversely, if there are better chances of freezing assets in another jurisdiction (for instance through a worldwide freezing order in the UK), it may be preferable to use Switzerland as an ancillary jurisdiction and to seek orders from the Swiss court in aid of foreign litigation, usually in the form of the recognition and enforcement of a foreign judicial decision.

2.2 Legal action in Switzerland

If, pursuant to the preliminary steps identified above, legal action is contemplated in Switzerland, one should then consider what kind of action is likely to be the most effective.

The successful attachment of the defendant's assets in Switzerland may lead to civil proceedings brought against that defendant in the Swiss courts on the ground that an attachment order creates such jurisdiction. However, depending on the circumstances of the case, it may be advisable to sue the defendant in another jurisdiction, provided that the claim is brought before the foreign court within the timeframe prescribed by Swiss law for perfecting a Swiss attachment order.

If a claimant has a choice between litigating the claim in the Swiss courts or abroad, he should carefully consider the pros and cons of each option, bearing in mind that civil litigation in Switzerland does not provide strong procedural tools to the claimant (such as disclosure of documents and cross-examination of witnesses).

If the circumstances of the case so allow, criminal proceedings may be contemplated. However, the claimant should bear in mind that there are a number of hurdles that need to be cleared, in particular the jurisdiction of the Swiss law enforcement authorities and the level of evidence required to persuade a public prosecutor to investigate the case. The decision to file a criminal complaint must not be taken lightly and, if it is taken, the claimant must ensure that the evidence backing up his allegations and suspicions is carefully assessed and sufficiently robust.

If those hurdles are cleared, the main benefit of criminal proceedings lies in the considerable discretionary powers that may be exercised by a public prosecutor to seize/freeze assets and to compel the defendant and other parties to disclose information and documents which may support the claimant's case. However, the claimant needs to consider that, contrary to civil litigation, he will not be in a position to control the conduct and the timeframe of criminal proceedings.

2.3 Outcome of legal action

If successful, civil litigation will lead to a favourable settlement or to a judgment awarding the claim. If the defendant's assets have been successfully attached, enforcement action will then be possible over those assets in accordance with the Federal Act on Debt Collection and Bankruptcy.

If criminal proceedings have been instituted, they may be resolved in various manners. In many cases where there is sufficient evidence of unlawful conduct, the public prosecutor may enter a summary penalty order against the defendant. Criminal charges may also be resolved through a trial or through so-called simplified proceedings whereby the defendant will acknowledge unlawful conduct in exchange for a milder penalty. Plaintiffs in the criminal action intervene in that process which may lead to a resolution of civil claims.

The trial court and in some instances the prosecuting authority may order restitution of proceeds of crime to the injured party or allocate the defendant's assets to the injured party by way of compensation of loss and damages.

3 Parallel proceedings: a combined civil and criminal approach

As indicated under Section 1 above, Swiss law provides for the possibility of bringing parallel

civil and criminal proceedings.

Based on the doctrine of civil tort, civil litigants may seek recovery or compensation before civil courts for the damage incurred.

Likewise, a plaintiff may, through the use of criminal proceedings, obtain disclosure of valuable information (in particular bank records) and the freezing of assets. The plaintiff may raise and seek the adjudication of civil claims in the context of criminal proceedings.

However, the plaintiff should exercise caution before asserting a civil claim in criminal proceedings, since that action will create *lis pendens* which will deprive the plaintiff of the possibility of bringing a similar claim against the same defendant in separate civil proceedings. A combined civil and criminal approach may be justified in situations where the determination of the claim and of its quantum is complex and thus more easily resolved through civil litigation. In such a situation, criminal proceedings may yield disclosure of vital information that will then be placed by the claimant before the civil court to optimise the chances of a successful outcome.

However, there are situations where the conduct of criminal proceedings may be sufficient to ensure the tracing and recovery of ill-gotten assets, since Swiss criminal law tends to protect the rights of injured parties. For instance, restitution of the proceeds of crime to the injured party takes priority over the confiscation of those assets in favour of the State.

Furthermore, the allocation of the defendant's assets (even if they are not the proceeds of criminal conduct) may be awarded to the injured party by way of compensation provided that the injured party's claim has been adjudicated by a court (civil or criminal) or recognised by the defendant.

Thus, the combination of the civil and criminal approach (or, conversely, the exclusive recourse to civil litigation or to criminal proceedings) will depend very much on a careful assessment of the specific facts and circumstances in each case.

4 Key challenges

Swiss civil litigation does not provide claimants with powerful tools that are available in common law jurisdictions. As noted above, there is no general disclosure/discovery in Switzerland, although the civil court has the power to compel the defendant or a third party to disclose specific documents in their possession if they are relevant to the case. Orders by the court to produce specific documents are infrequent. Nevertheless, a refusal by a party to submit a document requested by the other side may give rise to an unfavourable inference by the court.

There is no cross-examination of witnesses in Switzerland.

Thus, if the circumstances of the case permit, a claimant may prefer to litigate the claim in a jurisdiction which offers more robust tools.

These limitations do not apply however in criminal proceedings and a plaintiff/injured party may therefore opt to follow the criminal route which provides higher opportunities to trace, freeze and confiscate assets and to compel disclosure of information.

Another limitation of a civil law system such as Switzerland is the *in rem* nature of attachment orders which compels the claimant to identify beforehand assets of the defendant that are located on Swiss territory.

As noted above, UK worldwide freezing orders may be recognised in Switzerland under the 2007 Lugano Convention. However, there is no interim or injunctive relief available in Switzerland which will mirror the protective clauses of such orders, i.e. the provisions that allow the defendant to cover his legal costs and his living expenses. Thus, a claimant seeking the recognition of such orders in Switzerland will often opt for a declaration of bare enforceability without seeking other remedies from the Swiss court.

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

Fraud, asset tracing and recovery often occur in a multi-jurisdictional context.

The channels of judicial assistance may be used in support of domestic civil litigation. This includes in particular the service of judicial abroad and the obtaining of evidence from foreign jurisdictions. Such assistance is provided within the legal framework binding the requesting and the requested States mainly through the so-called Hague Conventions, in particular the Convention on Civil Procedure of 1 March 1954, the Convention on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters of 15 November 1965, and the Convention on the Taking of Evidence Abroad in Civil or Commercial Matters of 18 March 1970.

The same mechanisms are also used when the assistance of Switzerland is required in support of foreign proceedings.

Finally, the recognition and enforcement of foreign judgments is also possible in accordance with Art. 25-27 PILA or the 2007 Lugano Convention, as described under Section 1.4 above.

In criminal proceedings, international cooperation is provided for through the channels of mutual legal assistance in criminal matters. Cooperation is based on bilateral or multilateral treaties, such as the European Convention on Mutual Assistance in Criminal Matters of 20 April 1959.

In the absence of a specific treaty or convention binding the States, Switzerland will apply the provisions of its domestic law, the Federal Act on International Mutual Assistance in Criminal Matters of 20 March 1981.

It is noteworthy that unlike in common law countries, the process of collecting evidence of any kind (whether for civil or criminal proceedings) is considered under Swiss law as an official act akin to the exercise of a public power (*pouvoir public*), which falls within the scope of Art. 271 SCC if the evidence is collected for use in foreign judicial proceedings. In particular, the gathering, compiling and establishing of means of evidence (documents, witness depositions, written witness statements, etc.) all qualify as official acts as defined in Art. 271 SCC and may only be performed by Swiss authorities. The same applies if a person seeks to produce evidence in foreign proceedings that is not in his or her possession or under his or her control and must be gathered in Switzerland from a third party.

6 Technological advancements and their influence on fraud, asset tracing and recovery

Fraudsters are becoming increasingly sophisticated and adapt their approaches quickly. In recent years, new threats have arisen. Data breaches enable fraudsters to access personal information and take control of electronic devices and bank accounts.

This has forced institutions, and in particular banks, to take steps to implement technologies to prevent and detect risks of fraud.

These new technologies used by fraudsters have complicated the task of tracing assets. It has therefore become more common to call upon the services of companies specialised in international asset-searching techniques and using cutting-edge technologies.

We should note that the Swiss Federal Police (FedPol), as well as certain Cantonal police forces (e.g. Zurich), have set up special cyber-crime units to tackle cyber-crime. These units also cooperate on an international level with foreign police forces such as, for instance, through the channels of EuroJust.

7 Recent developments and other impacting factors

There have been two recent and significant legislative developments in Switzerland:

- Class actions: draft legislation is currently being considered for the purpose of enforcing claims regarding mass and disbersed damages. If approved, the bill will allow group action rights for the submission of monetary claims such as collective claims for

damages or surrender of profits. Such collective claims will require a written mandate by each injured party instructing the litigating entity to initiate the appropriate proceedings (the so-called "opt in").

The preliminary draft bill also proposes the introduction of collective settlement proceedings which will allow the defendant party to enter into a comprehensive agreement regarding the consequences of a breach of legal obligations with the organisation authorised to bring a group action. If the settlement is approved and declared enforceable by the competent court, it will bind all involved parties unless they declare their withdrawal from the collective settlement within a certain time period (the so-called "opt out").

- Recognition of foreign bankruptcy proceedings in Switzerland: as of 1 January 2019, the PILA Act has been amended to facilitate the recognition of foreign bankruptcy decrees in Switzerland. Former legal requirements for such a recognition have been eased. It is no longer necessary that the concerned foreign State should grant reciprocity to Switzerland. Further, the foreign bankruptcy decree no longer needs to be issued at the place where the debtor has its registered office; it may now also be issued at the place where the debtor effectively conducts its business, provided that the debtor's domicile or registered office was not located in Switzerland at the time when the foreign proceedings were opened.

Under the former rules, the recognition of a foreign bankruptcy decree always triggered the opening of the so-called ancillary bankruptcy proceedings in Switzerland to ensure the preferential payment of secured creditors and of privileged Swiss creditors out of the assets located in Switzerland. Under current legislation, the opening of ancillary bankruptcy proceedings in Switzerland will not always be necessary. Upon the request of a foreign bankruptcy trustee, no such ancillary bankruptcy shall be opened if no secured or privileged Swiss creditors have announced any claims and if a Swiss court determines that the claims of ordinary Swiss creditors have been adequately taken into account in the foreign proceedings. If no ancillary proceedings are required in Switzerland, the foreign bankruptcy trustee will have the power to transfer assets out of Switzerland and conduct legal proceedings in Switzerland; however, the trustee is not authorised to exercise acts of public authority or to adjudicate claims.

Paul Gully-Hart is a partner in Schellenberg Wittmer's dispute resolution group in Geneva, where he heads the white-collar crime and compliance group.

Paul is well versed in all aspects of common law and has developed a strong practice in complex litigation matters, including banking and commercial disputes that frequently involve an international component as well as multi-jurisdictional aspects. He is specialised in regulatory and compliance issues, corporate investigations, asset tracing and recovery, business crime defence work, and international mutual assistance in criminal and regulatory matters.

Some recent examples of Paul's expertise include assisting a major banking group in investigations conducted by Swiss public prosecutors on the basis of money laundering allegations targeting a former client of the bank and his investment adviser; and representation of a prominent Swiss industrialist and philanthropist prosecuted in Italy since 2002 in connection with an alleged intentional disaster. The case is of huge scale, involving cross-border issues and management of complex expert evidence.

paul.gully-hart@swlegal.ch

George Ayoub is a partner in Schellenberg Wittmer's dispute resolution, white-collar crime and compliance, and internal corporate investigations groups in Geneva.

His key areas of expertise and practice focus on white-collar crime, international mutual legal assistance, extradition, asset tracing and recovery, and internal corporate investigations. George is also specialised in regulatory and compliance issues.

George has acted as counsel for both individuals and corporate entities in criminal and administrative proceedings before cantonal and federal authorities and courts, including the Swiss Supreme Court.

George's recent expertise in white-collar crime matters include: representation of and assistance to a prominent businessman and his group of companies in relation to Swiss criminal investigations in the context of an alleged corruption scheme; and representation of a foreign sovereign fund and affiliated companies in Swiss criminal investigations targeting one of its former senior officers.

George is a member of the International Bar Association's anti-corruption, business crime and criminal law committees.

george.ayoub@swlegal.ch

Schellenberg Wittmer is one of the leading Swiss business law firms. Over 150 lawyers in Zurich, Geneva and Singapore advise domestic and international clients on all aspects of business law. The firm offers a comprehensive range of services from focused advice to project management, for local or foreign companies and high-net-worth individuals. Schellenberg Wittmer's Singapore office covers key jurisdictions and markets in the Asia-Pacific region, assisting clients in both inbound and outbound investments as well as in international arbitration.

www.swlegal.ch

Schellenberg Wittmer

United States

Joe Wielebinski
Winstead PC

Toby Galloway
Winstead PC

Matthias Kleinsasser
Winstead PC

Fraud, asset tracing and recovery always present challenges. Fortunately, in the U.S., the process is less problematic because we have the benefit of:

- established common law and statutory law designed to protect against fraud;
- well-developed case law interpreting the law;
- a well-trained and educated judiciary;
- adherence to the Rule of Law;
- effective criminal law enforcement authorities that assist with the pursuit of criminal wrongdoing; and
- a legal system that protects the parties' rights while providing effective relief to victims of fraud and other illegalities.

The system is not perfect, and there are often limitations or restrictions that make the pursuit of fraud difficult, time-consuming and expensive. Nevertheless, the U.S. legal system is admired as one of the most effective for combating fraud. The intent of this article is to give the reader a better understanding of the U.S. legal framework relating to fraud, asset tracing and recovery.

I Important Legal Framework and Statutory Underpinnings to Fraud, Asset Tracing and Recovery Schemes

The U.S. has federal jurisdictions and 50 states, plus the District of Columbia, Puerto Rico, and other districts and territories. In addition to consulting federal law, one must analyse the laws of the various other jurisdictions that could apply. The state and local systems are beyond the scope of this chapter, but you should review applicable state laws for any helpful claims or remedies.

A Fraud Causes of Action

1 Common Law Fraud

The most basic fraud claim is common-law fraud. Common law, or judge-made law, is the body of law in the United States derived from judicial precedent, as opposed to legal codes and statutes. The United States traces its common law history to England. In general, common-law fraud occurs when a party makes a false representation of fact to another party who relies on the representation and is injured as a result. (*See, e.g.*, *Vicki v. Koninklijke Philips Elecs., N.V.*, 85 A.3d 725, 773 (Del. Ch. 2014) (*citing* Delaware law); *Cromer Fin. v. Berger*, 137 F. Supp. 2d 452, 494 (S.D.N.Y. 2001) (*citing* New York law).) The representation must be material and the injured party must be unaware of its falsity. (*See, e.g.*, *Strategic Diversity, Inc. v. Alchemix Corp.*, 666 F.3d 1197, 1210 n.3 (9th Cir. 2012) (citing Arizona law).) Less commonly, a claim may exist based on fraud by non-disclosure, which occurs when a party fails to disclose material facts which the non-disclosing party has a legal duty to disclose. The injured party must rely on the non-disclosure and be injured as a result. (*See, e.g.*, *Bombardier Aero. Corp. v. SPEP Aircraft Holdings, LLC*, 572 S.W.3d 213, 219-20 (Tex. 2019) (citing Texas law); *Wallingford Shopping, L.L.C. v. Lowe's Home Ctrs., Inc.*, No. 98 Civ. 8462 (AGS), 2001 U.S. Dist. LEXIS 896, *43-44, 2001 WL 96373 (S.D.N.Y. Feb. 5, 2001) (*citing* Connecticut law).)

2 Statutory Fraud

U.S. federal and state laws contain various types of statutory fraud. These statutes were enacted to address fraud committed in the course of a particular type of transaction (*e.g.,* securities fraud or real estate fraud).

a) Securities Fraud:

The most significant securities fraud statutes are found in the Securities Act of 1933 (the "Securities Act") (15 U.S.C. §§ 77a *et seq.*) and the Securities Exchange Act of 1934 (the "Exchange Act") (15 U.S.C. §§ 78a *et seq).* The Securities and Exchange Commission has supplemented the anti-fraud provisions of the Securities Act and the Exchange Act with its own rules, which also provide causes of action. For example, S.E.C. Rule 10b-5, codified at 17 C.F.R. § 240.10b-5, supplements Section 10(b) of the Securities Exchange of 1934. For example, Section 17(a) of the Securities Act prohibits offering or selling securities using a device, scheme, or artifice to defraud (15 U.S.C. § 77q(a)(1)), while SEC Rule 10b-5 makes it unlawful to make an untrue statement of material fact in connection with the purchase or sale of a security (17 C.F.R. § 240.10b-5). Some causes of action in securities laws provide a private right of action, meaning that a private party may bring suit based on the statute. SEC Rule 10b-5 is one example. Other causes of action are available only to the government; e.g., claims under Section 17 of the Securities Act. (*See SEC v. Pocklington*, No. EDCV 18-701 JGB, 2018 U.S. Dist. LEXIS 227362, *42, 2018 WL 6843663 (C.D. Cal. Sept. 10, 2018) (stating that no implied private right of action exists for Section 17(a) claims).) In addition to the federal securities laws, states have adopted their own securities regulations known as "blue sky laws", many of which allow private rights of action for injured parties. (*See, e.g.*, Tex. Civ. Stat., Title 19, Art. 581-1 *et seq.*)

b) Other Types of Statutory Fraud:

States have enacted numerous statutes addressing fraud in various contexts. For example, Section 27.01 of the Texas Business & Commerce Code provides a cause of action and exemplary damages for a person injured by fraud in a real estate or stock transaction. All states have laws prohibiting the use of deceptive trade practices, including fraud. (*See, e.g.*, Cal. Bus. and Prof. Code §§ 17500 *et seq.*; 2019 Minn. Stat., Chapter 352D, § 325D.44 *et seq.*) Also, Title 18 of the U.S. Code, as well as the statutes of each state, make the commission of fraud a criminal offence in many contexts. (For example, using the mails to commit fraud is prohibited by 18 U.S.C. § 1341.)

c) Fraudulent Transfer Law:

The U.S. has a well-developed body of law permitting creditors to recover fraudulent transfers of money and other property. Most states have adopted the Uniform Fraudulent Transfer Act ("UFTA"), with minor differences existing between the statutes enacted by the states. (*See, e.g.,* Tex. Bus. & Com. Code §§ 24.001 *et seq.* (setting forth Texas's version of the Uniform Fraudulent Transfer Act).) The U.S. Bankruptcy Code also contains provisions allowing for recovery of fraudulently transferred property which are generally similar to the UFTA (11 U.S.C. § 548).

The UFTA allows for recovery of two types of fraudulent transfers. The first type – transfers made with actual intent to hinder,

delay, or defraud a creditor – are commonly referred to as actual fraudulent transfers (*see, e.g.,* Tex. Bus. & Com. Code § 24.005(a)(1)). Despite the name, fraudulent intent is not required so long as the transfer was at least intended to hinder or delay a creditor's collection efforts. Fraud is, by definition, secretive. The UFTA provides a non-exclusive list of factors (so-called "badges of fraud") the court may consider in determining whether a transfer was made with fraudulent intent (e.g., that the transfer was concealed) (Tex. Bus. & Com. Code § 24.005(b)). The second type of recoverable transfer is commonly referred to as a constructively fraudulent transfer. Constructively fraudulent transfers need not involve actual fraud, but merely require that the transferor received less than reasonably equivalent value for the property transferred. In addition, constructive fraudulent transfer law has a solvency element: the transfer must have been made while the transferor was insolvent, undercapitalised, or unable to pay its debts as they became due. (*See, e.g* ., Tex. Bus. & Com. Code §§ 24.005(a)(2), 24.006(a).) Constructive fraudulent transfer law protects creditors by discouraging a party with limited assets from transferring those assets away for less than reasonably equivalent value.

A creditor with a fraudulent transfer claim may sue both the initial transferee of the transferred property and any subsequent transferee. But a subsequent transferee who took the property in good faith and in exchange for value is immune from a fraudulent transfer suit. (Tex. Bus. & Com. Code § 24.009(b).) In this way, U.S. fraudulent transfer law balances protecting a creditor's right to recover property and protecting innocent third parties who took property without knowledge of the fraudulent transfer.

B Tools for Practitioners

1 Discovery

Practitioners seeking to trace and recover assets can use the extensive discovery process allowed in American litigation. Litigants may serve requests for production of documents, demand that adversaries answer sworn interrogatories, and depose witnesses. (*See, e.g.*, Fed. R. Civ. P. 30-34.) Third parties may be compelled by subpoena to provide testimony or produce documents. (*See, e.g.,* Fed. R. Civ. P. 45.) Some U.S. jurisdictions permit pre-suit discovery from third parties. But the U.S. lacks a uniform streamlined process such as the Norwich Pharamacal orders allowed in the U.K., which permit the requesting party to obtain a court order requiring a third party to disclose information or preserve assets or documents. The permissible scope of discovery is broad. Once a lawsuit has been filed and the defendant has appeared, the plaintiff can generally obtain discovery regarding any non-privileged matter that is relevant to a party's claims or defences and proportional to the needs of the case. Information need not be admissible in evidence to be discoverable. (*See, e.g.*, Fed. R. Civ. P. 26(b)(1).) Courts in the U.S. also generally prefer disputes to be resolved after discovery has been conducted, meaning that a plaintiff need not obtain and plead most of its evidence when it files its initial complaint. Some U.S. jurisdictions do require that certain claims be pled with particularity, including fraud claims. (*See, e.g.*, Fed. R. Civ. P. 9(b).) For these reasons, the discovery process may be the most potent tool for practitioners to uncover concealed assets. In limited circumstances, a party may conduct discovery prior to filing a lawsuit, though the extent to which pre-suit discovery is allowed varies significantly between U.S. jurisdictions. For example, Texas Rule of Civil Procedure 202 permits pre-suit discovery to investigate a potential claim, while Illinois Supreme Court Rule 224 generally allows pre-suit discovery only to identify potential defendants.

2 Injunctive Relief

A party concerned that someone may take steps to shelter or conceal assets should consider requesting injunctive relief. An injunction is

an equitable remedy under which a court orders the enjoined party to refrain from certain acts. Temporary injunctions (also called preliminary injunctions) operate to preserve the *status quo* until a case can proceed to trial. Temporary restraining orders remain in place for only a brief period (e.g., 14 days) until a request for a temporary injunction can be heard. Permanent injunctions permanently require the enjoined party to refrain from engaging in certain conduct.

A temporary injunction can serve as an important remedy for a party who suspects that another party is fraudulently transferring assets. The party should apply to the court for a temporary injunction preventing the other party from disposing of property without court permission. Although temporary restraining orders can often be obtained on an *ex parte* basis, temporary injunctions typically require an extended hearing on the following elements: (1) proof of an underlying cause of action (e.g., actual fraudulent transfer); (2) a probable right to recover on the underlying claim; (3) probable, imminent, and irreparable harm to the applicant if the injunction is not granted; (4) the injury that will occur if the injunction is not granted outweighs any harm that will result from granting the injunction; and (5) a showing that the injunction serves the public interest. (*Paulsson Geophysical Servs. v. Sigmar*, 529 F.3d 303, 309 (5th Cir. 2008); *Butnaru v. Ford Motor Co.*, 84 S.W.3d 198, 204 (Tex. 2002).) An injury is irreparable if the applicant cannot be made whole with an award of damages against the enjoined party (*Butnaru*, 84 S.W.3d at 204). If the enjoined party violates the injunction, it may be held in contempt of court and be subject to criminal and/or civil liability.

3 Receiverships

A more drastic equitable remedy is a court-appointed receiver. Under U.S. law, a receiver is a custodian who takes control of a business or enterprise, generally to preserve its value. Both federal and state courts may appoint receivers and litigants may file applications seeking their appointment. (*See, e.g.*, Fed. R. Civ. P. 66 (providing that an action in federal court in which the appointment of a receiver is sought is governed by the Federal Rules of Civil Procedure); *Brill & Harrington Invs. v. Vernon Savs. & Loan Ass'n*, 787 F. Supp. 250, 253 (D.D.C. 1992) (considering several factors in appointing a receiver, such as fraudulent conduct on the defendant's part and imminent danger of property being lost, concealed, or diminished in value); Tex. Civ. Prac. & Rem. Code § 64.001(a) (permitting a Texas court to appoint a receiver in several situations, including for an insolvent corporation or a corporation in imminent danger of insolvency, and further permitting a receiver to be appointed under the rules of equity).) The scope of a receiver's powers are established by court order, meaning that most courts have broad discretion to tailor a receiver's powers to a particular situation. (*See, e.g.*, Fed. R. Civ. P. 66 (providing that an action in federal court in which the appointment of a receiver is sought is governed by the Federal Rules of Civil Procedure); *Brill & Harrington Invs. v. Vernon Savs. & Loan Ass'n*, 787 F. Supp. 250, 253 (D.D.C. 1992) (considering several factors in appointing a receiver, such as fraudulent conduct on the defendant's part and imminent danger of property being lost, concealed, or diminished in value); Tex. Civ. Prac. & Rem. Code § 64.001(a) (permitting a Texas court to appoint a receiver in several situations, including for an insolvent corporation or a corporation in imminent danger of insolvency, and further permitting a receiver to be appointed under the rules of equity).) Typically, courts are inclined to appoint receivers only when the person running a business has engaged in fraud or the value of the business is in serious jeopardy.

4 Involuntary Bankruptcy

Involuntary bankruptcy may be an intriguing possibility for a party seeking to recover assets. Most bankruptcies in the U.S. are voluntarily filed by the debtor. Section 303 of the U.S. Bankruptcy Code, however, permits a

bankruptcy to be filed by one or more creditors holding claims that are not contingent as to liability or subject to *bona fide* dispute. (*See* 11 U.S.C. 303(b). A single creditor may file an involuntary bankruptcy proceeding if the creditor's claim exceeds $16,750; otherwise, three creditors with combined claims in the amount of $16,750 or more must sign the bankruptcy petition. *Id.* The minimum claim amount is periodically adjusted upward by the U.S. Congress when the Bankruptcy Code is amended.) If the bankruptcy is contested by the debtor, the court will hold a trial to determine whether an order for relief should be entered (meaning that the case will proceed) or the case should be dismissed (11 U.S.C. § 303(h)).

Filing an involuntary bankruptcy is a serious act and a petitioning creditor may be subject to damages and sanctions (including exemplary damages) if the petition is dismissed or filed in bad faith (11 U.S.C. § 303(i)). For a good faith creditor concerned about preserving or recovering assets, however, an involuntary bankruptcy has significant advantages. The debtor must prepare schedules of assets and liabilities and disclose pre-bankruptcy transfers of property, with all of these disclosures being signed under penalty of perjury (11 U.S.C. § 521(a)). If the court approves, the creditor may examine the debtor or third parties under oath and obtain production of documents to determine what happened to the debtor's assets. These examinations are referred to as Rule 2004 examinations, so named because they are authorised under Rule 2004 of the Federal Rules of Bankruptcy Procedure. These examinations are commonly granted and have been approvingly referred to as "fishing expeditions". Bankruptcy courts take fraudulent representations and omissions made in the course of a bankruptcy seriously and Title 18 of the U.S. Code makes bankruptcy fraud a federal crime. (*See, e.g.*, 18 U.S.C. § 157.) A bankruptcy trustee may file suit to recover fraudulently transferred property under Section 548 of the Bankruptcy Code (11 U.S.C. § 548; *see also* 11 U.S.C. § 544(b), which authorises the trustee to file suit based on state fraudulent transfer law to the extent a creditor could otherwise bring such a suit outside of the bankruptcy). Accordingly, under appropriate circumstances, involuntary bankruptcies can provide significant advantages to parties seeking to recover fraudulently transferred assets. For an example of a creditor successfully using an involuntary bankruptcy proceeding to enforce a judgment in light of alleged fraudulent transfers, *see In re Acis Capital Mgmt., L.P.*, 2019 Bankr. LEXIS 292 (Bankr. N.D. Tex. Jan. 31, 2019) (confirming involuntary chapter 11 plan) (full docket available at Case No. 18-30264).

5 Assistance to Foreign Tribunals (28 U.S.C. § 1782):

Section 1782 of Title 28 of the U.S. Code permits a U.S. District Court to order a person to provide testimony or produce documents to assist a foreign tribunal. The order may be issued upon request by the foreign tribunal or upon application of an interested party. Section 1782 is an important tool for litigants in non-U.S. proceedings to obtain testimony and information from persons located within the U.S.

II Case Triage: Main Stages of Fraud, Asset Tracing and Recovery Cases

The following is a general guide to typical stages of a U.S. proceeding based on a defendant's fraudulent conduct:

A Pre-Suit Investigation:

One should conduct as much pre-suit investigation as possible before filing suit. Frequently, only limited information can be obtained before filing. But at a minimum, a party should search public records (e.g., prior court filings, lien searches), which are accessible online. Internet searches and review of public social media accounts frequently turn up significant information that can later be used during lawsuit discovery to uncover fraudulent conduct or hidden assets. Parties may also consider hiring a private investigator or paying an internet asset search provider if the fees are reasonable. If the applicable jurisdiction allows for pre-suit discovery, those tools should also be considered. However, because many jurisdictions limit pre-suit discovery, the party should balance whether tipping off the suspected fraudster by requesting pre-suit discovery can be justified by the anticipated benefit from such discovery.

When considering what steps to take before filing suit, timing is critical. A party who suspects that its adversary is fraudulently transferring assets generally cannot afford to take a leisurely approach to litigation, particularly when assets can easily be moved. In such circumstances, a party should consider moving immediately for a temporary restraining order and temporary injunction to preserve the *status quo*.

B The Lawsuit:

A "traditional" lawsuit is the most commonly commenced proceeding, but receivership and involuntary bankruptcy proceedings can also be considered. If the defendant fails to appear in the lawsuit, the plaintiff should move for default judgment. (*See, e.g.*, Fed. R. Civ. P. 55.) If the defendant does file an answer, the parties then generally proceed to serve discovery. The broad scope of discovery, and the various discovery tools available in the U.S., are an excellent means to uncover fraud. If the plaintiff believes that money has gone missing and can obtain financial records, the plaintiff should consider retaining a forensic accountant to determine if funds were fraudulently transferred.

C Judgment Enforcement:

U.S. courts almost never permit a party to recover assets prior to a judgment being obtained. A party may obtain a temporary injunction preventing a defendant from transferring or disposing of assets. But a temporary injunction order is intended only to preserve the *status quo* prior to trial, not to permit a plaintiff to seize assets. Once a judgment has been obtained, however, the plaintiff is generally free to enforce it against whatever property it can locate belonging to the defendant. A defendant who wishes to appeal the judgment may be able to forestall enforcement while the appeal is pending. (*See, e.g.*, Fed. R. App. P. 8.) If the defendant does not appeal, if the judgment is not stayed pending appeal, or if an appeal is ultimately resolved in the plaintiff's favour, the plaintiff faces a daunting task: identifying assets sufficient to satisfy its claims. The plaintiff will usually serve post-judgment discovery requests to identify assets. Or, in some jurisdictions, the plaintiff may request an examination of the defendant, in which the defendant is required to submit to examination regarding the availability of assets to satisfy the judgment. Once the plaintiff has located assets, it can proceed to enforce its judgment against them, depending on the type of assets identified. Frequently, discovery will uncover fraudulent transfers by the defendant. In such case, the plaintiff can sue to recover the transfers.

III Parallel Proceedings: A Combined Civil and Criminal Approach

Parallel civil and criminal proceedings have proliferated in recent decades in the U.S. The U.S. Supreme Court acknowledged 50 years ago that parallel civil and criminal proceedings are proper and constitutional (*United States v. Kordel*, 397 U.S. 1, 11 (1970)). Such proceedings routinely arise where one federal agency has civil regulatory authority over a particular category of fraud (*e.g.*, the Securities and Exchange Commission (securities fraud), Commodity Futures Trading Commission (commodities fraud), Federal Trade Commission (consumer fraud)), while the Department of Justice has concurrent criminal jurisdiction over the same subject.

These complex situations raise a host of issues under the U.S. Constitution and other federal law. For example, invocation of the Fifth Amendment's privilege against self-incrimination has vastly different repercussions in the criminal context – where no adverse inference may be drawn from the invocation – versus the civil context – where an adverse inference can

be drawn. (*See*, *e.g.*, *Baxter v. Palmigiano*, 425 U.S. 308 (1976).)

A What Are the Benefits/Difficulties of a Combined Approach?

Parallel proceedings in which a private litigant seeks asset recovery while a government agency simultaneously pursues the fraudsters are also relatively common. These situations raise similar challenges and opportunities as in the parallel regulatory civil and criminal prosecutions.

One issue that may arise in such situations is where a stay of the civil proceeding is sought pending the criminal prosecution. If a plaintiff sues for fraud, and the government contemporaneously prosecutes the defendant for a crime arising from overlapping conduct, either the defendant or the government may move for a stay. Issuance of a stay will obviously delay any efforts to recover assets through the civil action.

If the defendant seeks a stay, he will argue that the civil action should be stayed until the criminal proceeding is concluded so that he does not have to choose between testifying (and thereby potentially waiving his Fifth Amendment privilege in the criminal case) and invoking the Fifth Amendment (thereby giving rise to an adverse inference in the civil action). If the government seeks a stay of the civil case, it will argue that the criminal defendant should not be permitted to avail himself of the more liberal civil discovery procedures for use in the criminal case.

These questions are highly fact-specific and courts do not automatically grant a stay on the request of either party. Generally speaking, the more the conduct at issue in the civil and criminal proceedings overlaps, the likelier it is that a stay will be granted. Courts also consider prejudice to the parties, delay, the public interest, and other relevant factors.

B Civil and Criminal Asset Recovery

There are a number of potential remedies in the civil context. The primary remedies in the criminal context (apart from incarceration) are asset forfeiture and restitution orders. The following is a brief overview of various civil and criminal remedies.

Federal Rule of Civil Procedure 64 authorises remedies relating to the seizure of persons or property – including arrest, attachment, garnishment, replevin, sequestration, and other similar remedies – to secure satisfaction of a potential judgment to be entered in the civil action (Fed. R. Civ. P. 64; *HMG Prop. Investors,*

Inc. v. Parque Indus. Rio Canas, Inc., 847 F.2d 908, 913 (1st Cir. 1988)). Obtaining these prejudgment remedies creates considerable leverage.

Other aggressive prejudgment relief includes temporary restraining orders and preliminary injunctions against further activity, freezing assets to prevent dissipation of investor proceeds, and receiverships. (*See* Fed. R. Civ. P. 64-66; 28 U.S.C. § 3103 ("Receivership").) A receiver is a person or entity appointed by a court to hold property that is subject to a dispute, whether the dispute concerns ownership or rights in the property or claims against the property's owner that might be satisfied from the property. A receiver is obligated to manage the property, to conserve it, and to prevent its waste. The receiver is authorised to receive rents and other income from the property, to collect debts, to bring or defend actions related to it, and to receive a fee for doing so. A receiver is subject to court supervision and responsible to the court for carrying out all orders regarding the property.

Asset freezes, orders appointing receivers, and related court orders may be enforced through civil or criminal contempt. Criminal contempt must be prosecuted by the government or the court, not the private plaintiff. Therefore, it is less useful as a method of recovery than civil contempt. Criminal contempt, unlike civil, involves punishment such as incarceration or fines for doing something prohibited by a court order. Civil contempt typically involves

the failure to do something required by a court order. In civil contempt, the remedy is designed to be compensatory, not punitive. So, if a defendant dissipates assets or refuses to tender property to the receiver, the plaintiff or receiver can compel compliance by showing, by clear and convincing evidence, that the defendant violated an order and is therefore in contempt. If the contemnor does not purge the contempt, he may be incarcerated pending compliance with the court order.

In criminal cases, the primary means of asset recovery are forfeiture and restitution. Criminal forfeiture is the taking of real or personal property by the government due to its relationship to criminal activity, such as when the property is used in the commission of a crime or was obtained through criminal activity. Civil forfeiture is similar to criminal forfeiture except it is brought against the property itself as an *in rem* action.

Restitution means payment by an offender to the victim for the harm caused by the defendant's misconduct. Courts are empowered (and often required) to order convicted criminals to pay restitution.

There are considerable disadvantages to relying on criminal remedies in asset recovery. First, the criminal authorities may not prosecute the offence. Of course, the victim may assist the government and encourage prosecution, but there are no guarantees. If the government does prosecute, it bears the burden of proving guilt beyond a reasonable doubt, a much higher burden than the preponderance-of-the-evidence standard in civil cases. Finally, the government will have to distribute the assets seized or restitution paid. In practice, this may take many years. Because of these disadvantages, judgment creditors and other victims of fraud should almost always pursue their own asset recovery in the U.S. through civil proceedings.

C How Does the U.S. View Private Prosecutions?

Private prosecutions, meaning criminal prosecutions conducted by private attorneys or laymen, have long been disfavoured in the U.S., to the point of extinction. This stands in contrast to the U.K., where private prosecutions have flourished in recent years. Indeed, the U.S. has not permitted private prosecutions in over 150 years except in exceedingly rare and unusual circumstances. For instance, a federal district court may appoint a private attorney to prosecute a criminal contempt of court if the executive branch refuses to prosecute. (*Young v. United States ex Rel. Vuitton Et Fils, S.A.*, 481 U.S. 787 (1987).) In practice, this situation is extremely uncommon and not susceptible to prediction or planning. Federal statutes confer the exclusive power to prosecute crimes in the name of the U.S. on the Attorney General and his delegates. (*See* 28 U.S.C. §§ 516, 519; *United States v. Nixon*, 418 U.S. 683, 693 (1974) ("the Executive Branch has exclusive authority and absolute discretion to decide whether to prosecute a case").) Thus, private prosecutions are not a realistic option for asset recovery.

IV Key Challenges

Among the key challenges is the cost to pursue and recover assets from fraudsters. Cost can be an impediment to deserving victims and must be managed whenever fraud and asset recovery are being pursued. In addition, there are challenges in exporting recovery efforts outside the U.S. In many "less established" jurisdictions, there is an *ad hoc* and lengthy process for judgment enforcement, discovery is limited or unavailable and the recovery of assets is chaotic and unpredictable. Some jurisdictions do not have the necessary legal framework, experienced and trained judiciary or respect for the Rule of Law to facilitate the recovery of assets for fraud victims. While the concept of a Model Law for cross-border insolvencies undertaken by UNCITRAL has been successful, recent UNCITRAL meetings have focused on the need for a Model Law for

asset recovery. Although this is commendable, it may take many years to implement.

Other challenges unique to the U.S. are outlined below:

A Attorneys' Fees:

Unlike many jurisdictions, the default rule in the U.S. is that each party bears its own attorneys' fees. This is not to say that attorneys' fees are never recoverable in U.S. litigation if a statute so provides. (*See, e.g.*, Tex. Civ. Prac. & Rem. Code § 38.001 (providing for recovery of attorneys' fees in certain types of cases, such as breach of contract cases).) Parties to a contract are also free to specify how attorneys' fees should be allocated in light of a dispute. Without a contractual or statutory basis for fees, however, each party must pay its own fees. Mounting attorneys' fees can prove to be a significant hurdle for a plaintiff pursuing a lawsuit and attempting to enforce a judgment.

B Tracing Commingled Proceeds:

One of the difficulties frequently faced by a party attempting to recover fraudulently transferred funds is how to identify those funds when they are commingled with other money in a bank account. U.S. courts have applied several tests to address this issue, with the most widely applied test being the lowest intermediate balance rule. This test assumes that the owner of a bank account preserves fraudulently obtained money for the benefit of defrauded victims. Funds from other sources are presumed to be withdrawn first. Only if the balance of the account drops below the amount of fraudulently obtained funds are the victims' funds presumed to be gone. (*See Blackhawk Network, Inc. v. Alco Stores, Inc. (In re Alco Stores, Inc.)*, 536 B.R. 383, 414 (Bankr. N.D. Tex. 2015) (explaining application of lowest intermediate balance rule).) An additional problem arises if funds are spent and new funds are subsequently deposited. Courts are split on whether victims' funds can be replenished.

C Exemptions:

A common obstacle to judgment recovery in the U.S. against an individual person (as opposed to an entity) is state property exemption laws. The United States Bankruptcy Code also contains federal exemptions for debtors filing for bankruptcy which differ from state exemptions, which debtors filing bankruptcy in some (but not all states) can choose to use (11 U.S.C. § 522(d)). The goal of exempt property laws is to ensure that creditors do not leave individual debtors destitute. The breadth of exemptions varies significantly by state, with states such as Texas providing robust protection with respect to real property used as a domicile and other states providing only a limited homestead exemption. (*Compare* Tex. Prop. Code § 41.001 *with* Ark. Code, Chapter §§, § 16-66-210.) In addition, some states wholly exempt retirement accounts, certain life insurance policies, annuities, and other financial instruments, meaning that a plaintiff facing a debtor that has properly structured his or her limited assets may be out of luck. In most states, a transfer of an exempt asset cannot constitute a fraudulent transfer because the UFTA (in effect in most U.S. jurisdictions) excludes exempt assets from its scope. (*See, e.g.*, Tex. Bus. & Com. Code § 24.002(2).)

V Cross-Jurisdictional Mechanisms: Issues and Solutions in Recent Times

Obtaining assistance in the U.S. on cross-jurisdictional matters involving fraud and asset recovery can be challenging even for the experienced practitioner. This is not because of the lack of available tools or an unwillingness to assist, but rather, determining what mechanisms are available and best suited for your situation. The online resources of the U.S. Department of Justice and Department of State are an excellent starting point. (*See e.g.,* U.S. Asset Recovery Tools & Procedures: A Practical Guides for International Cooperation (2017).)

The insolvency process can be one of the most effective tools to combat fraud (Brun, Jean-Pierce and Silver, Molly.2020. Going for Broke: Insolvency Tools to Support Cross-Border Asset Recovery in Corruption Cases. Stolen Assets Recovery series. Washington, DC: World Bank doc: 10.1596/978-1-4648-1439-9). As such, it is appropriate to discuss Chapter 15 of the U.S. Bankruptcy Code, which addresses cross-border insolvencies. Chapter 15 is designed to promote cooperation between the U.S. courts and parties of interest and the courts and other competent authorities of foreign countries involved in cross-border insolvency cases while providing for the fair and efficient administration of cross-border bankruptcies (11 U.S.C. § 1501. See Chapter 15 – Bankruptcy Basics: Ancillary and Other Cross-Border Cases (www.uscourts.gov)).

A Chapter 15 case is commenced by a "foreign representative" filing a petition for recognition of a "foreign proceeding" (11 U.S.C. § 1504). The U.S. court is authorised to grant preliminary relief upon the filing of the petition for

recognition (11 U.S.C. § 1519). Upon the recognition of a foreign main proceeding, the automatic stay and other important provisions of the Bankruptcy Code take effect within the U.S. The foreign representative is also authorised to operate the debtor's business in the ordinary course (11 U.S.C. § 1520).

Chapter 15 is the principal means for a foreign representative to access U.S. federal and state courts (11 U.S.C. § 1509). Upon recognition, a foreign representative may seek additional relief from the bankruptcy court or from other state and federal courts and is authorised to initiate a full (as opposed to ancillary) bankruptcy case (11 U.S.C. §§ 1509, 1511). In addition, the representative is authorised to participate as a party in interest in a pending U.S. bankruptcy and to intervene in any other U.S. case where the debtor is a party (11 U.S.C. §§ 1512, 1524).

Chapter 15's use has increased since its adoption and there is now an established body of case law. Moreover, more countries have adopted some corollary of the Model Law on which Chapter 15 is based. Importantly, Chapter 15 is being used more frequently in cross-border fraud and corruption cases. Accordingly, Chapter 15 must be considered as a formidable weapon in appropriate fraud, asset tracing and recovery efforts.

VI Technological Advancements and Their Influence on Fraud, Asset Tracing and Recovery

While there is no substitute for hard work, technology can be vitally important in pursuing claims for fraud. A party may obtain up to date information regarding assets and individuals from public and non-public databases. Comprehensive online resources include BlackBookOnline.info, Accurint.com and TLO.com. Social media has become a useful tool for investigators to find out what might otherwise be considered private information from numerous sites like Facebook, LinkedIn, Twitter and Instagram.

Various products and providers offer assistance in managing data and discovery, which can often involve millions of documents. Technologies like Greylist Trace (greylisttrace.com), while new, appear promising and can provide information on banking relationships that help to focus investigative resources. Technology will continue to play an important, and indeed, critical role in fraud, asset tracing and recovery in the future.

Conversely, technology is being used more and more by fraudsters, often making recovery more difficult and challenging. The best example is the fast-paced developments regarding cyber-crimes and fraud involving cryptocurrencies.

VII Recent Developments and Other Impacting Factors

One development that is getting attention is the extra-territorial application of U.S. law, especially as it relates to avoidance actions. The Second Circuit Court of Appeals recently addressed this issue in the context of the Madoff Ponzi scheme (*In re Picard*, 917 F.3d 85 (2d Cir. 2019)). In declining to rule that the presumption against extra-territoriality was applicable, the Court determined that the Trustee could recover a domestic transfer to foreign transferees (so-called "feeder funds") under the avoidance powers of the Bankruptcy Code (*RJR Nabisco, Inc. v. European Cmty.*, 136 S.Ct. 2090,

2100 (2016) ("absent clearly expressed congressional intent to the contrary, federal laws will be construed to have only domestic application.")). As the Court noted, under a contrary ruling, fraudsters would enjoy an easy way to protect their ill-gotten gains (*Id.* at 26-27). When this ruling is combined with a prior decision in Madoff on the extra-territorial application of the automatic stay (Van der Hahn, D. and Wielebinski, J.; *Extraterritoriality Arguments Ruled Extraneous: Second Circuit Permits Trustee to Recover Fraudulent Transfers from Foreign Recipients*, International Bar Association. *Insolvency and Restructuring International*, Vol. 13 No. 2, September 2019), it may be a harbinger of future expansion of the reach of the Bankruptcy Code in international fraud cases (*Picard v. Maxam Absolute Return Fund, L.P.*, 474 B.R. 76, 84-85 (2012)).

Joe Wielebinski is a member of Winstead's business restructuring/bankruptcy practice group. For more than 30 years, his practice has concentrated on bankruptcy, creditors' rights and financial restructuring, and he is active throughout the United States in a variety of complex restructuring, insolvency and bankruptcy matters and related litigation.

Joe has represented numerous victims in matters involving complex financial fraud, theft, money laundering and other white-collar crimes. He has also served as a Federal District Court receiver at the request of the SEC in cases involving national and cross-border fraud schemes.

Joe is the Executive Director Emeritus of ICC FraudNet, a London-based, invitation-only organisation consisting of lawyers throughout the world who have significant experience in complex commercial fraud and offshore asset identification and recovery. Joe is a member of FraudNet's Advisory Board, the International Bar Association, International Association for Asset Recovery, American Bankruptcy Institute and Turnaround Management Association.

jwielebinski@winstead.com

Toby Galloway is co-chair of Winstead's securities litigation & enforcement practice group. He practices in the areas of white-collar defence, governmental and internal investigations, and complex securities and commercial litigation. Toby previously served as an attorney with the United States Securities and Exchange Commission for over 11 years. During his last four years at the SEC, Toby was the chief trial counsel for the Commission's Fort Worth Regional Office.

Toby routinely practices before federal and state securities regulators, and self-regulatory organisations. He also represents clients before the DOJ and other regulatory and law enforcement agencies. Toby represents public companies, audit committees and special committees, hedge funds, private equity funds, asset managers, broker-dealers, registered investment advisers, accountants and lawyers, and other institutions in government and internal investigations, securities law enforcement, and litigation. A longtime member of the American Bar Association, he serves on the ABA regional white-collar criminal justice sub-committee.

tgalloway@winstead.com

Matthias Kleinsasser is a member of Winstead's business litigation, white-collar defense and business restructuring/bankruptcy practice groups. His practice encompasses all aspects of commercial litigation in state and federal court, with an emphasis on bankruptcy-related litigation, securities litigation, securities enforcement proceeding defence and white-collar defence.

Matthias has significant experience representing debtors, creditors, and trustees in virtually all aspects of business bankruptcy proceedings. He has also represented clients before the Securities and Exchange Commission and FINRA.

Matthias began his legal career in Fort Worth as a law clerk to former U.S. bankruptcy judge D. Michael Lynn. Prior to joining Winstead, he practiced with large law firms in Dallas and Fort Worth, as well as with a respected business bankruptcy boutique firm.

mkleinsasser@winstead.com

Who's moving

Who's buying

Who's selling

Who's growing

IBR INTERNATIONAL BUSINESS REPORTS

Current and strategic insights into key business sectors worldwide

A new online news and analysis service from the publishers of the International Comparative Legal Guides (ICLG.com) and Commercial Dispute Resolution (CDR-News.com), International Business Reports offers daily online reporting on global business and commerce, along with thought leadership and opinion from leading industry insiders on the issues that really matter.

Contact us

To discuss your potential role as an information provider, advertiser or sponsor, get in touch to begin the conversation:

Andrea Rubino, Head of Content Strategy, International Business Reports

andrea.rubino@glgroup.co.uk

+44 203 890 8981

+44 747 596 9281

ICLG.com/ibr

@IBR_GLG

International Business Reports is published by: glg global legal group

ARRIVING ONLINE AND IN PRINT IN SUMMER 2020

CDR
Commercial Dispute Resolution

ESSENTIAL INTELLIGENCE:

The Belt & Road Initiative

cdr-news.com

ICLG.com