ICC FraudNet
COMMERCIAL CRIME SERVICES
est. 2004

GLOBAL REPORT 2021

International Developments and
Perspectives in the field of
Fraud, Financial Crime and Asset Recovery

Acknowledgments

Many individuals and organisations have been of great assistance in the writing, editing and production of the inaugural FraudNet Global Report. The Editor first wishes to thank FraudNet's Members and Strategic Partners who have authored and co-authored articles for inclusion in this publication, as well as their colleagues and staff who have assisted them. FraudNet's unparalleled international reach and subject expertise in fraud and asset recovery are well captured in this Report, and it is testament to the collective energy of the group that such wide-ranging insights were provided for this Report from so many countries, particularly in these unprecedented times.

The Editor secondly wishes to thank Mr Peter Lowe, Executive Secretary of FraudNet for his support from the inception of this project right through to publication. His operational assistance, and acute understanding of the expertise and resources available within FraudNet has been greatly valued during the collation of papers. Further thanks are owed to Mr Michele Caratsch and Mr Babajide Ogundipe for their help throughout the strategic stages, and work in convening and being part of, along with Mr Peter Lowe, a very supportive Editorial Board. The Editor wishes to thank all members of the Editorial Board – Mr Bobby Banson, Mr Shaun Reardon-John, Mr Rodrigo Callejas, Mr Waseem Azzam, Mr Christopher Redmond and Mr John Greenfield – for their time, guidance and energy for this project. Gratitude is also extended to Mr Bruce Horowitz, whose support as an Assistant Editor has been significantly valued during the review and editorial stages, and also Mr Andrew Witts for his guidance.

Finally, the Editorial Board wishes to thank all Members, Strategic Partners and Staff of FraudNet for their continued support and collaboration in making this Report possible.

Contents

Foreword

This, the first FraudNet Global Report emerged from discussions of members at our Beirut meeting in October 2019. Following the decision to elect us as co-Executive Directors, members may have thought that we had to be kept busy. One of the things that emerged were thoughts about the need to develop a more academic element to the network. Given that the focus of our members is more practical in nature, aimed at providing results for clients, this was a move in a slightly different direction. Consideration was given to participating in programmes with educational institutions, and this thinking resulted in a meeting in January 2020 with Professor Barry Rider OBE, the Founder of the annual Cambridge International Symposium on Economic Crime and sometime Fellow, Dean and Tutor of Jesus College, Cambridge, amongst his many accomplishments. At the time, the existence of a new disease reported to have originated in Wuhan, China, was known, but nobody at that meeting had any notion of what was to come.

Professor Rider introduced us to Dr Dominic Thomas-James, who agreed to be the Editor of a journal that would feature articles on developments related to our practice areas from our members and Strategic Partners, as well as from leading academics engaged in research relating to economic crime, risk, financial regulation and compliance, and who were authors of key academic texts in the field.

The explosion of the new disease into something that left no part of the world untouched was not foreseen. Had it not occurred, this Report would nevertheless have been produced. The pandemic prevented FraudNet members, Strategic Partners and invited guests from meeting in Nairobi and Miami in 2020. Had we been able to hold these meetings, doubtless some of the material contained here would have been shared there. Whilst the Report did not come about as a result of the pandemic, what we are experiencing most certainly influenced some of its contents. The certification of vaccines, which started in December 2020, holds out hope that the fears, restrictions and risks related to travel will have dissipated by the time the 2022 Report is published.

We thank all the contributors, not just for providing such valuable material, but for doing so in good time and thereby relieving the Editor of chasing them holding a big stick. This augurs well for future editions.

We hope that readers will find the articles that follow informative and stimulating. Please share the Report widely and do not hesitate to engage our contributors directly or through our indefatigable Executive Secretary, Peter Lowe. We cannot end these few words without expressing our thanks to Dominic Thomas-James and to the other members of the Editorial Board for their work on this, our first, FraudNet Global Report.

Babajide Ogundipe *Michele Caratsch*

16th December 2020

Babajide Ogundipe
***Partner,* Sofunde Osakwe Ogundipe & Belgore**
Lagos, Nigeria
e. boogundipe@sooblaw.com
t. +234(1)4622502

Michele A. Caratsch
***Partner,* Baldi & Caratsch**
Zurich, Switzerland
e. mcaratsch@bclaw.ch
t. +41-44-250 2525

Executive Summary

Fraud and financial crime are among the greatest inhibitors to the stability and prosperity of organisations, institutions and economies around the world – in both developed and developing jurisdictions alike. Fraud is the crime to which most people are likely to fall victim. However construed, be it sophisticated and complex commercial frauds, insider dealing, market manipulation, money laundering, bribery, terrorism financing or tax evasion, these are ever-developing, transnational threats to which meaningful and innovative thinking is required in response. While an ethos of "shared values, shared approaches" underpins the global anti-economic crime framework, particularly vis-à-vis money laundering and financial regulation, a one-size-fits-all approach often omits important contextual challenges across different jurisdictions.

For lawyers and investigators, only a more nuanced approach taken to the subject of fraud, financial crime and asset recovery will enable us to understand and properly articulate what the real challenges are at international, regional and domestic levels – both practically, and theoretically. Thereby, more meaningful and practical cooperation and collaboration can be facilitated.

In recent years, financial crime has been an increasingly regular subject in the news media. It has been seen in successive breaches of confidential data from law firms in the offshore world (such as the Bahamas leaks, the Panama and Paradise papers) and from enforcement authorities and regulators (such as the FinCEN files). Cases are increasingly high-profile involving some of the world's most well-known institutions. In terms of enforcement efforts, new civil and criminal tools are rapidly being designed and deployed beyond traditional recovery mechanisms or use of the criminal justice system – including deferred prosecution agreements to deal with complex international bribery allegations and AML breaches against large financial institutions, as well as new mechanisms such as unexplained wealth orders being used to target suspicious wealth of politically exposed persons, or those involved in serious crime.

While the mechanisms of case disposal, recovery or restitution have advanced, so too have the abilities of criminals to utilise innovative methods to perpetrate misconduct and conceal their illicit gains. These are impacting on insolvency and bankruptcy proceedings, and increasing the complexity of asset structuring and transaction chains. As the Covid-19 pandemic has acutely demonstrated, cyber-fraud and related misconduct is increasing. So too are the abilities to utilise under-regulated crypto-assets while systems of law around the world make their mind up about the nature of such 'property' and its regulation. Further, bad actors are utilising advancing technologies to perpetrate wrongdoing, and conceal or transact assets in non-traditional ways. Of course, the other side of this is that financial technologies are assisting practitioners and

investigators exponentially with recovery efforts, as well as transnational enforcement operations, information sharing, cooperation and mutual assistance.

Just as we are experiencing new and innovate threats, practitioners and the professions are faced with increasing regulatory and legislative obligations. Further, international financial and business centres, particularly 'offshore' markets, appear subject to growing, and perhaps disproportionate, pressure to change their models and comply with standards which are not yet global norms.

The Inaugural FraudNet Global Report 2021 draws upon the collective knowledge and experience-driven insights of its Members and Strategic Partners – all leaders in their interrelated fields of practice and who are at the forefront of some of the world's most high-profile, legally impactful and sensitive asset recovery cases involving fraud and related misconduct. The Report showcases thought-pieces, briefings and analyses from across the globe. Its aims are to strengthen the research and intellectual arm of the world's leading asset recovery lawyers' network, and to provide contemporary insight to existing and potential clients about some of the most pertinent issues facing our field and the type of subjects the Members and Strategic partners regularly encounter in their work.

Articles encompass a useful mix of case studies, theoretical discussions, and practical solutions-based insight. They cover a range of themes of timely importance, including developments in criminal and civil asset recovery initiatives such as economic substance requirements, beneficial ownership and corporate transparency, 'offshore' issues, fraud and insolvency, cybercrime and security, evidential and ethical considerations, unexplained wealth and account freezing orders, forged commodities, crypto-assets and their regulation, and forensic analysis. Practical illustrations and examples, particularly from the different regions represented in the report, adds context to complex and developing areas of law. The Report also includes articles from leading academics associated to FraudNet, who are engaged in ongoing research in the field.

The articles also provide comment, analysis and evaluation of some recent landmark legal judgments and their practical implications, enactment of new legislation and regulatory obligations. It also considers how technological solutions can assist clients in asset recovery, as well as casting practical predictions about their application and scope. Drawing upon the authors' individual professional experiences, useful learning outcomes and implications are proffered.

The Covid-19 pandemic has created an environment of dangerous opportunity, which is acknowledged across many of the papers in this Report. It is hoped that the articles are of utility and interest to existing and prospective clients and associates of the ICC FraudNet network, as well as provide valuable contributions to important and ongoing debates in the field. In this regard, it is also hoped that the Report will be of wider use to legislators, policymakers, investigators, researchers and scholars alike seeking to better enhance their understanding and contemporary

awareness of important developments in this field across the globe, many of which are covered insightfully and analytically in these papers.

Publications in this field are hardly lacking, however this Report is rather unique as it demonstrates individual insights of practitioners but also the broad experience of the network – which is its value proposition as the world's leading asset recovery lawyers' network. It is the Members and Strategic Partners' united belief that mutual collaboration at the transnational level can be of significant utility when assisting the victims of fraud and economic crime as they seek recompense in complex circumstances, often with transnational elements.

It is hoped that the readers of this Report find the papers herein most useful and insightful.

Dr Dominic Thomas-James

Dr Dominic Thomas-James

Editor, FraudNet Global Report

e. dominicthomasjames@cantab.net

Part I

Criminal and Civil Asset Recovery Initiatives

Asset Recovery Initiatives – A New Toolbox for Prosecutors

Kate McMahon

Abstract

In this article, Kate McMahon, a partner at the firm Edmonds Marshall McMahon, discusses recent developments in English law regarding suspicious wealth and recovering the proceeds of crime. By reference to various new statutory powers, including Account Freezing Orders and Unexplained Wealth Orders, set against the backdrop of the U.K.'s proceeds of crime framework, the author discusses how these new tools have been applied in English cases and reviews both their effectiveness and some of the concerns associated with them.

Background

In the second half of the 20th century, prosecutors' powers to recover the proceeds of crime expanded gradually. Asset-seizure laws were first introduced after a drug-trafficking case in 1978, known as 'Operation Julie'. In this case, the House of Lords held that existing laws could not be used to strip "*drug traffickers of the total profits of their unlawful enterprises.*"[1] In practice, this meant that the courts were unable to confiscate some £750,000 of criminal profits.[2] This unsatisfactory outcome led Parliament to introduce a confiscation regime under the Drug Trafficking Offences Act 1986 – although this legislation only applied to drug dealers initially, it was ultimately applied to a range of offences.[3]

Since the turn of the century, however, there has been a proliferation of new powers available to criminal prosecutors to assist with asset recovery. This acceleration is encapsulated by the enactment of the Proceeds of Crime Act 2002 ('POCA 2002' or the 'Act'). This Act, labelled by some as draconian, does have some of the world's toughest laws on the tracing and freezing of ill-

[1] *R v Cuthbertson* [1980] 6 WLUK 138
[2] "Proceeds of Crime Bill – Explanatory Notes", *House of Commons*, 18 October 2001, available at: <https://publications.parliament.uk/pa/cm200102/cmbills/031/en/02031x--.htm> last accessed 13 October 2020
[3] "Ill-gotten gains – police are hitting criminals harder in the pocket and keeping some of the proceeds", *The Economist*, 8 October 2009, available at: <https://www.economist.com/britain/2009/10/08/ill-gotten-gains >last accessed 13 October 2020

gotten gains. By way of background, the Proceeds of Crime Bill was introduced on 18 October 2001. At Parliament's Second Reading, the Minister for Police, Courts and Drugs, John Denham, described the legislation in the following terms:

> *"The Bill is about taking the profit out of crime… Traditionally, the criminal justice system has been much better at convicting criminals than at depriving them of their wealth. Far too many defendants pass through the criminal justice system with little or no effort being made to deprive them of the benefit that they have derived from their crimes. The Bill says that people should not be able to enjoy the proceeds of criminal activity. They should not enjoy the trappings of wealth when that wealth is built on the misery of victims or activities that damage and exploit society."*[4]

In line with these stated aims, the Act expanded asset-retrieval powers considerably, allowing courts to seize virtually anything owned by someone who had been convicted of a crime and deemed to have a "criminal lifestyle". When the Act came into force, Part 5 was particularly controversial – that is because it created a civil recovery regime, permitting the seizure of assets where no conviction was possible because, for example, individuals remained sufficiently distant from the commission of the crimes or because they had left the country. The most pervasive criticism in relation to Part 5 was that seizing assets before conviction disturbs the presumption of innocence, as well as, of course, property rights.

Notwithstanding this criticism, asset-seizure powers have extended even further in the last decade. For example, deferred prosecution agreements ('DPAs') were introduced in 2014 by the Crime and Courts Act 2013. These agreements are made under the supervision of a judge and allow organisations to avoid being prosecuted, provided they meet certain conditions. Therefore, it is now possible for the Serious Fraud Office ('SFO') to recoup the proceeds of crime through a DPA, without the need to actually prosecute. This is a powerful new tool. Additionally, the Criminal Finances Act 2017 (the 'CFA 2017') introduced Account Freezing Orders ('AFOs'), Account Forfeiture Orders ('AFORs') and Unexplained Wealth Orders ('UWOs'). The CFA 2017 was enacted to bolster the proceeds of crime regime, following the first global Anti-Corruption Summit in London, in May 2016. London was, and still is, seen to be home to one of the world's major financial markets. At the relevant time, the Home Office also considered the London property market to be unusually exposed to financial crime.[5]

Arguably, however, these new legal tools go too far and have unintended consequences that outweigh their benefits. For example, in relation to DPAs, some argued that this was the beginning of the "Americanisation" of corporate crime enforcement and that the integrity of British justice was being compromised.[6] Before analysing the efficacy of these legal tools and whether they go too far, it is worth exploring why asset-seizure powers have become fiercer in the last decade.

---

[4] "Proceeds of Crime Bill – Order for Second Reading read", *Hansard Commons Sitting*, 30 October 2001, available at: <https://api.parliament.uk/historic-hansard/commons/2001/oct/30/proceeds-of-crime-bill#S6CV0373P0_20011030_HOC_277> last accessed 13 October 2020

[5] "Criminal Finances Act – Overarching Impact Assessment", *Home Office*, 20 June 2017, available at: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/621192/Impact_Assessment_-_CF_Act_Overarching.pdf> last accessed 13 October 2020

[6] Joanna Dimmock, Jonathan Pickworth and Tom Hickey, "Deferred Prosecution Agreements 5 Years On – the Americanisation of UK Corporate Crime Enforcement", *White & Case*, 10 May 2019, available at:

For one, interviews conducted by the Home Office with drug offenders suggest that many organised criminals fear losing their assets far more than jail time. In other words, these new asset recovery powers are an effective deterrent. The interviews also showed that many drug offenders perceive prison as an "occupational hazard" and that the threat of losing assets and earnings is far more persuasive.[7]

Next, the seizing of convicts' assets is popular with the public and provides the police and prosecuting agencies with an additional income stream. However, concerns have been raised about the impact of these incentives – namely, that they encourage prosecuting agencies to pursue wealthy criminals, rather than those who do the most damage to society. There is much talk of this in the United States, where law enforcement has been criticized for "policing for profit".[8] This is, undoubtedly, less of a concern in the UK because the proceeds of crime are split between various organs of the state – half goes to the Home Office and the other half goes to the police, enforcement agencies and the courts under the Asset Recovery Incentivisation Scheme. Notwithstanding all the reasons in favour of the new toolbox of asset recovery powers, persuasive concerns have also been raised. This presents an important question: have these new measures, on balance, improved England's asset retrieval regime, or have they gone too far?

The new toolbox of powers

Account Freezing Orders

AFOs are one new power that have been added to the SFO's arsenal. They were introduced by section 16 of the CFA 2017, which inserted new sections into POCA 2002. Broadly speaking, AFOs allow for the freezing and subsequent forfeiture of funds held in bank and building society accounts. Since being introduced, there has been a surge in the number of applications for AFOs by law enforcement agencies, such as the City of London Police ('COLP'), HMRC and the SFO. The National Crime Agency ('NCA') also deploys this power regularly – for example, in 2019 they were granted freezing orders in respect of eight bank accounts containing a sum in excess of £100 million.[9] The appeal of AFOs to prosecuting bodies is clear – this power enables law enforcement agencies to target wealth linked to criminality that is held in a bank account. In other words, the contents of banks accounts can now be frozen and confiscated in the same way as large sums of cash, which were traditionally seen as the hallmark of criminality.

There are various other reasons why AFOs have been popular among law enforcement. Not only can an application be made before the Magistrates' Court, the minimum balance in the

<https://www.whitecase.com/publications/alert/deferred-prosecution-agreements-5-years-americanisation-uk-corporate-crime> last accessed 15 October 2020.

[7] "Ill-gotten gains – police are hitting criminals harder in the pocket and keeping some of the proceeds", *The Economist*, 8 October 2009, available at: <https://www.economist.com/britain/2009/10/08/ill-gotten-gains> last accessed 13 October 2020

[8] "Scrounging for coppers – Police in Britain want to keep more of the loot they confiscate", *The Economist*, 19 January 2017, available at: <https://www.economist.com/britain/2017/01/19/police-in-britain-want-to-keep-more-of-the-loot-they-confiscate> last accessed 13 October 2020

[9] "£100m Account Freezing Orders are largest granted to NCA", *National Crime Agency – News*, 14 August 2019, available at: <https://www.nationalcrimeagency.gov.uk/news/100m-account-freezing-orders-are-largest-granted-to-nca> last accessed 13 October 2020.

relevant account need only be £1,000. By contrast, an application for a UWO must be made in the High Court and the value of the property held must be more than £50,000.[10] Additionally, the evidential threshold for securing an AFO is low. There is no requirement for a criminal investigation to have commenced and an application may be made if the enforcement officer (for example, a COLP officer) has reasonable grounds for suspecting the matters in s.303Z3(2) of POCA 2002. This section provides:

> *(2) The relevant court may make the order if satisfied that there are reasonable grounds for suspecting that money held in the account (whether all or part of the credit balance of the account)—*
>
> *(a) is recoverable property, or*
>
> *(b) is intended by any person for use in unlawful conduct.*

The Court will then evaluate and decide whether there are reasonable grounds for that suspicion. Reasonable grounds for suspecting a fact means that the fact is suspected[11] and that there are objectively reasonable grounds for that suspicion[12]. As you will understand, "reasonable grounds for suspecting" is not a high threshold. This threshold does not require any fact to be proved, even "on a balance of probabilities" (the civil standard), and it is likely to be a lower threshold than the "good arguable case" formula that must be met in order to obtain an interim freezing injunction.[13] While in strict legal terms the applicant for an AFO bears the burden of proof, in practice the account holder has been expected to provide some sort of innocent explanation if he or she wants to avoid the freezing of their funds. Given the low threshold for the granting of an AFO, staying silent on the funds under investigation to avoid them being frozen (the "less is more" strategy) is unlikely to work in a respondent's favour.

Arguably, however, this new procedure goes too far. AFOs are effectively a civil tool and avoid the need to prove allegations to the criminal standard. According to some, this means the respondent loses "*crucial safeguards normally present in a criminal trial*", undermining the robustness of British justice.[14] To be sure, the ability to freeze bank accounts on such a low threshold may put individuals in a tricky position – asking an account holder to explain the provenance of all his funds and explain all outgoing transactions is arguably too onerous.[15] Additionally, as summed up by Aziz Rahman, "*Parliament's reasoning that the Magistrates' Court was the appropriate forum for these powers is also a concern*".[16] By contrast, UWOs are applied for in the High Court and restraint orders under POCA are applied for in the Crown Court. It is questionable to leave AFOs within the remit of the

---

[10] Nicola O'Connor, "Increasing Use of Account Freezing Orders", *Bird & Bird LLP*, July 2020, available at: <https://www.twobirds.com/en/news/articles/2020/uk/increasing-use-of-account-freezing-orders> last accessed 2 October 2020

[11] *O'Hara v. Chief Constable of the Royal Ulster Constabulary* [1997] AC 286

[12] *ARA (ex parte Jamaica)* [2014] UKPC 1 per Lord Hughes at [19]

[13] *The Niedersachsen* [1983] 1 WLR 1412

[14] Richard Fisher QC and Nichola Higgins, "Account freeing orders: at what cost?", *Doughty Street Chambers*, 10 December 2019, available at: <https://insights.doughtystreet.co.uk/post/102fvn0/account-freezing-orders-at-what-cost> last accessed 2 October 2020

[15] Aziz Rahman, "Account freezing orders: why we can expect more from them", *Rahman Ravelli*, 26 March 2019, available at: <https://www.lexology.com/library/detail.aspx?g=1ad343bd-93c3-4707-abae-86ce00ffad48> last accessed 2 October 2020

[16] Ibid

Magistrates' Court, which often fails to apply the rigour (not to mention the expertise) of the senior judiciary. An article published by Doughty Street Chambers highlights a risk that leaving AFOs to the Magistrates creates – that is, the "grab first investigate later" mentality, which has the power to inflict serious reputational and commercial damage on legitimate companies.[17]

Unexplained Wealth Orders

The UWO, introduced by the CFA 2017, also warrants close attention. This new tool was the government's response to difficulties in identifying suspects' source of wealth, which is required for civil recovery proceedings.[18] In their 2016 Impact Assessment Report, the Home Office explained that the UWO would create a new investigative power and assist in building evidence for non-conviction-based asset recovery. The explanatory notes to the Criminal Finance Bill 2016 also gave context on why this was important – enforcement authorities were struggling to obtain sufficient evidence for asset freezing proceedings under POCA 2002, especially where international cooperation was required.[19]

UWOs target specified property and the wealth used to acquire this property where such wealth is disproportionate or its source dubious. It places an onus on the subject of the order (the respondent) to explain the source of their wealth. Although UWOs are not available to private prosecutors, they are, nevertheless, a powerful investigatory tool and can be granted in relation to any property that has a value of more than £50,000. Although UWOs are granted on the basis of a relatively low threshold, the 2020 case *NCA v. Baker & Ors.* [2020] EWHC 822 (Admin) warrants attention. This High Court case dealt with a UWO and sheds some light on what an applicant must prove. Having considered other authorities, the judge said the following:

> *"The use of complex offshore corporate structures … is not, without more, a ground for believing that they have been set up, or are being used, for wrongful purposes, such as money laundering. There are lawful reasons – privacy, security, tax mitigation - why very wealthy people invest their capital in complex offshore corporate structures … Of course, such structures may also be used to disguise money laundering, but there must be some additional evidential basis for such a belief, going beyond the complex structures used."*[20]

Since they became available, the UK has only seen a handful of UWOs. Although the properties subject to UWOs have had a tremendous cumulative value, the NCA has only achieved one forfeiture to date, and this was through a settlement. On 7 October 2020, the NCA announced it had seized just over £9.8 million worth of assets (from 45 different properties). The settlement also meant a discontinuance of their investigation. That said, it is undeniable that UWOs are a powerful investigatory tool as they can compel a respondent to disclose details of his private life and financial situation. The *Baker* case is instructive on this point and highlights that from the

[17] Richard Fisher QC and Nichola Higgins, "Account freeing orders: at what cost?", *Doughty Street Chambers*, 10 December 2019, available at: <https://insights.doughtystreet.co.uk/post/102fvn0/account-freezing-orders-at-what-cost> last accessed 2 October 2020

[18] Jonathan Grimes and Ed Smyth, "Unexplained Wealth Orders: An overview of the regime to date", *Kingsley Napley*, 7 October 2020, available at: <https://www.kingsleynapley.co.uk/insights/blogs/criminal-law-blog/unexplained-wealth-orders-an-overview-of-the-regime-to-date> last accessed 14 October 2020

[19] "Criminal Finances Bill – Explanatory Notes", 12 October 2016, available at: <https://publications.parliament.uk/pa/bills/cbill/2016-2017/0075/en/17075en03.htm> last accessed 13 October 2020

[20] *NCA v. Baker & Ors.* [2020] EWHC 822 (Admin) at [97]

respondent's perspective, it can be advantageous to provide information voluntarily and take a collaborative approach. In this case, the three UWOs were discharged and the NCA were refused permission to appeal.

In summary, given their relative newness, it is difficult to ascertain the effectiveness of UWOs and AFOs. Broadly speaking, however, these powers seem to be a necessary and proportionate response to modern day crime. Those suspected of criminality do not always deal in cash anymore and the ability to interrogate the source of someone's wealth and the use of funds in bank accounts is simply the law's way of catching up with the 21st century. As criminal enterprise adapts, so too must the legislation seeking to rout it out.

Freezing cryptocurrency

To end, it's worth touching on another power that has been made available to prosecutors in the last 5 years – the ability to freeze crypto-assets (otherwise known as cryptocurrency). The proliferation of cryptocurrencies has created new opportunities for criminals to carry out high value heists. CipherTrace, a blockchain forensics company, has reported that losses from cyber-crime amounted to $4.52 billion in 2019. This represented a 150% increase from 2018.[21] As with all fraud, those who have been defrauded want to recover what is theirs and more victims of cyber-crime are requesting proprietary injunctions and freezing orders through the courts.[22]

The granting of court orders in respect of cryptocurrency has brought with it a particular issue, namely, is cryptocurrency even capable of being the subject of freezing orders and proprietary injunctions? In order for the courts to grant such orders, the claimant must show that the asset in question is personal property. However, classifying cryptocurrency in classical English law terms has proved problematic – is it a right, property or something else?[23] Although cryptocurrency is still not defined in statute, recent developments have helpfully clarified its legal status.

In November 2019, a group of barristers called the UK Jurisdiction Task Force ('UKJT') published a Legal Statement on Cryptoassets and Smart Contracts (the 'Legal Statement').[24] According to the Legal Statement, cryptocurrency is legally equivalent to property and the unique features of crypto-assets – "*intangibility, cryptographic authentication, use of a distributed transaction ledger, decentralisation, rule by consensus*" – do not prevent these assets from qualifying as property. The Legal Statement provided much needed clarity in this area and its analysis has been upheld in the English courts. For example, *AA v Persons Unknown* [2019] EWHC 3556 confirmed that cryptocurrency is property and noted that it is possible for this kind of asset to be the subject of freezing orders and proprietary injunctions.

---

[21] "Cryptocurrency Anti-Money Laundering Report, 2019 Q4", *CipherTrace*, January 2020, available at: <https://ciphertrace.com/wp-content/uploads/2020/02/CipherTrace-CAML-2019-Q4-20200220.pdf> last accessed 2 October 2020

[22] "Is Cryptocurrency Property?", *Edmonds Marshall McMahon*, May 2020, available at: <https://www.emmlegal.com/publications/is-cryptocurrency-property/> last accessed 11 January 2021

[23] Marc Jones, "Time to clarify the legal status of cryptocurrencies?", *Stewarts Law LLP*, 31 October 2019, available at: <https://www.stewartslaw.com/news/legal-status-of-cryptocurrencies/> last accessed 13 October 2020

[24] "Legal Statement on Crypto-assets and Smart Contracts", *UK Jurisdiction Taskforce*, November 2019, available at: <https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf> last accessed 3 October 2020

Cryptocurrencies are unique assets and it's not surprising their legal status has exercised lawmakers. Now that cryptocurrency has been definitively classified as property, the issue becomes *how* it should be frozen. Unlike traditional currencies, which are held in conventional bank accounts, cryptocurrencies are decentralised – as such, the freezing of crypto-assets is more complex than simply serving a worldwide freezing order on a bank. However, as evidenced by *Liam David Robertson v Persons Unknown* [unreported], court orders can, in fact, be served on coin exchanges. In this case, the claimant obtained an order in relation to Coinbase UK Limited, a UK domiciled crypto-exchange, helping him to obtain a $1,100,000 settlement.[25]

Conclusion

To conclude, recovering ill-gotten gains is a dynamic, complex area – this reflects the fact that criminality and the ways to hide criminal proceeds are continuously evolving. The proliferation of cryptocurrency and crypto-fraud, as well as the law's response to this new threat, illustrates this point. As discussed at some length, there has also been a proliferation of new powers available to prosecutors. Although controversial, POCA 2002 and the CFA 2017 are prominent examples of good practice in the area of asset recovery. These pieces of legislation were carefully crafted to keep pace with the evolving criminal landscape – this approach is essential for any asset recovery regime that hopes to be effective and have longevity.

[25] Syedur Rahman, "Freezing Crypto-assets", *Rahman Ravelli*, 5 December 2019, available at: <https://www.rahmanravelli.co.uk/articles/freezing-cryptoassets/> last accessed 2 October 2020

About the Author

Kate is a founding Partner of Edmonds Marshall McMahon, the UK's premier private prosecution firm, specialising in high value fraud. She specialises in serious, international fraud, asset recovery, large scale investigations and perverting the course of justice proceedings. She is typically instructed by corporates, hedge funds and HNW's in commercial fraud matters. Prior to founding Edmonds Marshall McMahon, Kate prosecuted for the Serious Fraud Office (SFO) where she worked as a senior lawyer on some of the UK's largest criminal prosecutions, including the "Innospec" case. This was the first global settlement in the UK and involved systemic corruption by a UK/USA company in Iraq and Indonesia. The case resulted in a US$12.7 million fine in the UK and a US$14.1 million fine in the USA and successful prosecutions of the Company Directors and employees.

Kate has also prosecuted a number of high-profile, high-value international "boiler room" frauds operating across a number of countries, involving thousands of victims. Kate also has significant experience in the area of confiscation and has also successfully conducted many large-scale fraud trials, including the famous "transit thefts" of pharmaceuticals in transit from EU factories to wholesale dealers in the UK. Kate is known for her incisive analysis and strategic vision, having had conduct of large fraud, corruption and trademark cases. She is highly regarded by her clients and has a reputation for being extremely determined and driven in all her cases. She has been described as an "outstanding prosecutor" who provides "intellectual leadership". She is praised for her "high intelligence, tactical acumen and great client care skills."

Kate McMahon
Partner, Edmonds Marshall McMahon

katemcmahon@emmlegal.com
+44 (0)20 7583 8392

Edmonds Marshall McMahon

Standing Up to Government Corruption: Access to Justice through Civil Asset Recovery and Private Funding as Alternatives to Public Investigation and Forfeiture

James Pomeroy

Abstract

In this article, James Pomeroy of Grant Thornton examines corruption in the public sector. At a time of increased global uncertainty, the author outlines important background on government or 'official' corruption, and reinforces the devasting effects that corruption has both in the context of developed countries, but also developing states in which unaccountability and corruption is systemic. The paper discusses civil recovery of the proceeds of official corruption, outlining the key stages and the multi-stakeholder approaches required to maximise the recovery of value. It also discusses the insolvency process as a machine of recovery. It also addresses the important question of funding in the context of the risk-value balance, set against other political, economic and social constraints often seen in such cases.

Introduction

Corruption is the abuse of power by those in positions of trust, influence, or authority, for personal benefit at the cost of the broader society. It robs nations of their financial, social, and environmental well-being, it pervades the psyche of citizens and leads to all kinds of decay, widening the divide between the powerful and the powerless.

Left unbroken, the cycle of corruption continues for generations, leaving apathy and a blunted sense of hope to those who live in a corrupt society. Corrupt behaviour is nothing new and has been the subject of considerable international focus for decades. Professor Paul Heywood observed that despite the heighted attention, "citizens across the world simply don't believe that such initiatives have had any effect […] the real danger is that corruption becomes seen as a norm within any political process."[1] In 1997, the United Nations recognized the seriousness of the impact of

[1] Heywood, Paul M., 2017, "Why we need to understand better how and why corruption occurs, and what we can do to address it", available at: https://www.thebritishacademy.ac.uk/blog/why-we-need-understand-better-how-and-why-corruption-occurs-and-what-we-can-do-address-it/

corruption across societies, undermining the rule of law and leading to violations of human rights, adopting the United Nations Convention Against Corruption[2].

Why stand up to corruption? Surely, the obvious and overly simplified answer must be to make a better life for all, to elevate the standard of living across a population, and to bring wrongdoers to justice. All are more easily said than done. What can be done, and how? These may not prove to be the rhetorical or unanswerable questions they first appear. There are paths to recovery, albeit slow and long term in nature. These include implementing, monitoring, and enforcing governance regimes and shifting societal norms and expectations about the behaviour of public officials.

Cultures of corrupt states are so imbued with cynicism and acquiescence that bad actors can carry on their schemes with bold impunity, caring little about scrutiny or its likelihood. Interrupting the cycle demands a shift away from apathy and indifference. There may be more immediate pathways to change, either in a tangible way by finding and recovering stolen assets and corrupt wealth, or in a less palpable one, through the psychological benefit to society from seeing corrupt actors brought to justice.

The Cost of Corruption

There are obvious, large scale, immediate economic and financial costs of corruption. They include the value extracted directly from the state and converted into personal benefit in the usual ways such as luxury homes, expensive automobiles, yachts, planes, and other hard goods. Unfortunately, glitzy, high-profile hard assets often over-shadow the negative downstream effects on society. Smaller scale corruption, like the bribes paid by ordinary citizens to ensure that everyday life carries on uninterrupted, takes on a more mundane appearance and revolves around issues such permits being issued, goods being retrieved from customs, and official forms being stamped. While relatively smaller individual transaction values, these aggregate to something larger than the sum of their parts and contribute to a weakening of society by virtue of the nature of act, rather the amount. A death by a thousand cuts.

More significant pay-to-play schemes involve high level collusion between the private and public sector. Bribery and corruption on this scale involves trillions of dollars extracted from public coffers and divided amongst the participants in these schemes. In 2018, UN Secretary General Antonio Guterres estimated that corruption costs the global economy more than $1 trillion paid in bribes, and another $2.6 trillion across other forms of corruption.[3]

According to the United Nations Development Programme's Sustainable Development Goal 16, corruption, bribery, and tax evasion account for more than $1.25 trillion annually in developing countries alone, enough to lift the populations of those countries above the poverty threshold of only $1.25 per day[4] for at least six years[5].

---

[2] United Nations Convention Against Corruption, Preamble, 2003

[3] UN News, December 2018, available at: https://news.un.org/en/story/2018/12/1027971

[4] US$1.25 per day was the international poverty line used by the World Bank until it was increased to US$1.90 per day in 2015. The update reflected changes in cost of living and exchange rates from when the previous line was set but it preservers the same approximate purchasing power.

[5] United Nations Development Programme, Sustainable Development Goal Target 16, available at: https://www.undp.org/content/undp/en/home/sustainable-development-goals/goal-16-peace-justice-and-strong-institutions/targets.html

High level corruption is often played in plain view and is widely known or speculated about by the general public, who usually have no individual power to take action. This contributes to public angst and damages collective spirit. Schemes like cartels, infrastructure construction fraud, illegal political campaign financing, and systemic circumvention of government contracting requirements (if they even exist) have a broader desaturation effect on entire economies, suppressing otherwise functional consumer and commercial markets and lowering the quality of life.

As awareness, acceptance or indeed the expectation of corruption grows and a collective indifference spreads throughout society, an inherent distrust in the government and the wider political system takes root. Tax collection in corrupt states suffers as low-level functionaries demand bribes for one favour or another. Even more concerning is the negative impact on the willingness of individuals to pay tax into a corrupt system at all, further depriving the state of its ability to generate much needed revenue. Why should good citizens contribute to a dysfunctional institution?

The higher the levels of perceived and actual corruption, the more difficult it can become to attract outside investment, impeding economic growth, reducing employment rates, and stifling innovation.[6] The empirical evidence is still developing and the degree to which foreign investment is impacted can vary depending on the definition scope of corruption that is applied in the research. For example, political forms of corruption may have less of an effect on the foreign investment decision than bribery, which can result in serious criminal and financial repercussions in the investors' home jurisdiction.[7] Even so, despite that there are many variables to consider, studies have found that economies that implement effective measure to control corruption and improve the quality of their institutions and rule of law may attract a greater inflow of foreign investment.[8]

A stunted economy with devolving expectations becomes fertile ground for a population with little hope of success from honest hard work alone. It becomes open to activity that would otherwise be unacceptable from a moral standpoint as a trade-off for ensuring the prosperity of one's family.

A Disproportionate Impact

The World Bank Group recognizes that corruption has a disproportionate impact on certain countries and demographics. Increased costs, reduced services, and cuts to social programmes hit poorer and more vulnerable populations the hardest[9] as these populations do not have the same choices as wealthier ones do[10]. As a percentage of household income, routine bribes demanded by the police or a public official take food of the tables of poorer families. The UN recognized that "corruption hurts the poor disproportionately by diverting funds intended for development,

[6] C.D. Howe Institute (2001), citing Wei 1999; Gray and Kaufman 1998; Gupta, Davoodi, and Alonso-Terme 1998; and Mauro 1995.
[7] DeNolf, Bert. The Impact of Corruption on Foreign Direct Investment (2008), The Journal of World Investment & Trade, Vol. 9, Issue 3
[8] Epaphra, Manamba. (2017). The Effect of Corruption on Foreign Direct Investment: A Panel Data Study. Turkish Economic Review. 4. 19-54. 10.1453/ter.v4i1.1234.
[9] C.D. Howe Institute (2001), citing Wei 1999; Gray and Kaufman 1998; Gupta, Davoodi, and Alonso-Terme 1998; and Mauro 1995.
[10] World Bank, Combating Corruption - https://www.worldbank.org/en/topic/governance/brief/anti-corruption accessed October 28, 2020.

undermining a Government's ability to provide basic services, feeding inequality and injustice, and discouraging foreign aid and investment.[11]

In dramatic contrast to the overwhelmingly negative impact of corruption on society, however, bribes paid by the wealthy are a much lower proportion of their income or wealth as compared to the poor. A Transparency International survey of more than 63,000 respondents found "that it is the poor who are most often confronted with requests for bribes, in wealthy and poor countries alike." It also found that endemic, mandatory "extortion hits low-income households with a regressive tax that saps scarce household resources."[12]

It is reasonable to infer that optional, high-value bribes paid by the wealthy tend to serve to enhance political connection or social status. For example, wealthy families can choose to pay astounding sums to propel their children to the front of admissions queues at elite universities, as illustrated by the recent Varsity Blues college admission scandal in the United States. In 2019 the US Federal Bureau of Investigation uncovered a scheme in which 49 high net worth and celebrity parents of high school-aged children paid more than $25 million in bribes to ensure their children's acceptance into elite US colleges and universities.[13] Some families paid more than $500,000 for the certainty of admission to highly prestigious institutions. The voluntarily complicit payor of a bribe is rewarded with greater access and opportunity to participate in financial success, whereas the vulnerable population may be forced to make crucial moral choices simply to survive.

Spiralling Economic and Social Decline

Economic desaturation deprives the state of funding for social programmes, educational systems, public infrastructure, healthcare, recreational services, and so on. These institutions and programmes deteriorate, the quality of service suffers, and public perception and trust declines. Public expectation gets lower and lower. But the costs reach wider than merely financial and economic loss. Rule of law and political stability are perverted when the political elite are seen to be living with impunity from the proceeds of corruption.

Political or ethnic divisions widen, and for some their only natural recourse is perceived to be voting in election. In countries where corruption is endemic, a pattern of changes in government each election cycle or two emerges wherein the incoming party, having run on a platform of change, undertakes a half-hearted lookback at the incumbent party, resolving to clean up and bring transgressors to justice. All too often though, promises to bring justice (or retribution) of the predecessor regime inevitably remain unfulfilled and the cycle of corruption continues unbroken. Public faith in political institutions reduces. Half-hearted efforts to investigate corruption unsupported by the highest levels in government are simply left unattended to stagnate or are met with endless legal and public challenge, eventually forgotten as the next scandal finds its way into the public eye.

---

[11] United Nations Convention Against Corruption, Foreword, 2003

[12] Transparency International, Global Corruption Barometer 2007, available at: https://www.transparency.org/en/press/20071205-poor-families-hit-hardest-by-bribery-even-in-rich-countries-finds

[13] US Department of Justice, 2019, available at: https://www.justice.gov/usao-ma/pr/arrests-made-nationwide-college-admissions-scam-alleged-exam-cheating-athletic

Development Funding

Failure to control widespread corruption and to implement basic governance has been shown to negatively impact development funding from other countries. In 2001, the C.D. Howe Institute examined the effectiveness of the Canadian International Development Agency's (CIDA) development Aid. Among its findings was that "CIDA should coordinate with other donors while focusing on the effectiveness of its own aid." Coordination is useful to resolving the highly complex issues surrounding corruption and poor governance that detracts from aid effectiveness.[14] In 2008, CIDA made aid effectiveness and accountability for development results a keystone of its development priority to reduce global poverty. In its action plan introduced that year, CIDA committed, by 2010-2011 to focusing 80% of its bilateral aid over the following 3 years to just 20 countries, emphasising effectiveness, accountability, and transparency in an effort to maximise aid effectiveness .[15]

Good governance is something of a subjective term. In their long-running research series prepared for the World Bank, Kaufman, Kraay, and Mastruzzi (1999) concluded that "there is a strong causal relationship from good governance to better development outcomes such as higher per capita incomes, lower infant mortality, and higher literacy"[16]. They later posit that there is a positive relationship between good governance and positive development outcomes.

The World Bank, through its commission of the Kaufman et al study, have advanced indicators of good governance as aggregated in their "6 Worldwide Governance Indicators"[17], among which includes "Control of Corruption". States which take active steps to embrace change and incorporate better governance stand a greater chance of reaping the rewards from development funding through both immediate increase in funding and the long-term benefit of more effective development outcomes. Naturally, it is in every state's best interest to maintain or increase the flow of development funds from international contributors.

Breaking the Cycle

Breaking the cycle of corruption demands sweeping macro-level change and the implementation and enforcement of prevention and detection policies. Enhanced governance and the establishment of robust anti-corruption and whistle-blower legislation underpins a shift in public psychology and behaviour as signals of real intent. Institutional change takes significant time and political commitment to accomplish. Profound, permanent change encounters many obstacles that require commitment and political will from the highest level. Absent that endorsement, experience shows that the cycle can too easily continue, despite the public will to break it. The public

[14] C.D. Howe Institute (2001), citing Wei 1999; Gray and Kaufman 1998; Gupta, Davoodi, and Alonso-Terme 1998; and Mauro 1995.
[15] Government of Canada, CIDA's Aid Effectiveness Action Plan (2009-2012, available at: http://www.publications.gc.ca/collections/collection_2011/acdi-cida/CD4-68-2010-eng.pdf
[16] The Worldwide Governance Indicators, Kaufman, Kraay, Mastruzzi, 1999
[17] The Worldwide Governance Indicators, Kaufman, Kraay, Mastruzzi, 2010 - WGI cover over 200 countries and territories, measuring six dimensions of governance starting in 1996: voice and accountability to citizens, political stability and lack of violence, government effectiveness, an efficient regulatory framework, the rule of law, and control of corruption. The aggregate indicators are based on several hundred underlying variables.

vote that fuels the partisan election back and forth is not enough. The voices of the powerless are not enough, but their will is a necessary first step.

Call to Action

Seeds of change are sown by citizens and civil servants who refuse to accept as a societal norm that public officials, when presented with corrupt opportunity will act in their own interests rather than the interests of the state. In 2015-2016, Guatemala, Lebanon, Brazil, and Malaysia saw large public demonstrations against corruption and impunity.[18] Progress is slow. Civil servants and functionaries in corrupt institutions quite often, understandably, turn a blind eye to corruption so as to keep their livelihoods in economies that have been devastated. These actions enable systemic corruption and must be addressed. But there must be alternatives for these members of society – who, otherwise, would be forced to sacrifice their livelihoods when those in power around them are living in luxury.

Nations can stimulate change through the development of public policy aimed at preventing and detecting corruption, establishing frameworks that enable independent oversight and governance, and implementing measures to actively monitor and enforce adherence to public policy. This includes taking action where necessary to reinforce the consequences of breaching public trust. These models are critically important for a long-term recovery and shift in public motivation and the empowerment of those affected by corruption to break the status quo. Advancement of robust public policy and culture change are critical to the long-term emergence from a state of capture. However, these are long-term solutions and do not address corrupt activity in the near-term.

To supplement and emphasise commitment to the long-term policy positions and push for a more immediate impact, states need to take action to deter and deprive corrupt actors of the fruits of their actions, to fight against impunity. Illicit gains are often well hidden using professional advisors to help corrupt actors create sophisticated, highly complex international corporate and financial structures, requiring the state to look to comparably sophisticated private professional firms for guidance and strategy advice to penetrate those structures.

The war against corruption plays out over countless battles, each calling for perseverance and the will to overcome the actions taken by politicians, civil servants, public and private sector entities, and private individuals to obfuscate the proceeds of their actions. These actors must be pursued and made to turn over the cash, bank accounts, real and personal property they have accumulated from their graft.

Chapter V of the UN Convention Against Corruption sets out a fundamental framework for asset recovery and Article 53 establishes measures designed to improve international cooperation and facilitate cross border asset recovery. These include requiring adopting nations to permit foreign states to establish property claims within their jurisdictions, to take measures that would allow the domestic court to issue orders to pay damages or compensation that would be effective when enforced by a foreign state, and, to recognise foreign states' claims to ownership of property which is the proceeds of an offence.[19] Turning a blind eye or staging investigations that go nowhere simply

[18] Larsson, Naomi, "Anti-corruption protests around the world - in pictures" https://www.theguardian.com/global-development-professionals-network/gallery/2016/mar/18/anti-corruption-protests-around-the-world-in-pictures
[19] United Nations Convention Against Corruption, Chapter V, 2003.

contributes to the spiral that leads to failed statehood and enduring suffering by its citizenry. The measures introduced by the Convention serve to level the playing field be establishing pathway to recover assets that have been secreted in foreign jurisdictions.

Civil or Criminal Recovery

As public sentiment shifts and a call for change is heard, certain immediate objectives that drive actionable initiatives must be considered. For example, governments and societies at large will consider whether criminal action is preferred over civil claims. Public and political objectives can be at odds with each other when the political benefits are viewed to be more important by a new government than financial recovery through civil proceedings.

The quick political win through criminal charges or implications of fraud or corruption against members of the former government can be higher profile and have wider political ramifications than a long and drawn out civil legal battle to deprive that same official of their financial gain. Criminal repercussions that reach the higher levels of corrupt structures can be effective signals that change is happening. The quick fix of a high-profile criminal conviction used solely as a political manoeuvre may be viewed as exactly for what it is, and the short-term political benefit ultimately gives way to a new wave of corruption.

By contrast, a well-designed civil asset recovery strategy, making effective use of the various legal and financial investigation tools that are available, which may also include the criminal process, can have the dual benefit of shining a light on the predecessor's transgressions and recovering value that was lost to officials and beneficiaries of the corrupt regime.

When civil asset recovery is carried out with skilful public relations against well-defined targets and is sponsored by well-intentioned high-level government officials, recovery of value back into the economy can help to bring lasting change. In May 2020, after a six-year civil recovery process, Nigeria recovered over $300 million of value laundered by the former Abacha regime through structures in the United States and Jersey, Channel Islands. The recovered funds have been ringfenced to support indigent Nigerians and to expedite important infrastructure projects.[20]

Successfully tackling grand corruption can accomplish the desired financial recovery that can be so beneficial to society and it can also achieve the punitive element against wrongdoers which may partially satisfy both the general public and the desire for political win.

Funding the Recovery of Corrupt Proceeds

Throwing good money after bad. This is the mantra of any victim of fraud and it is often heard from the governments of victim states as well. Naturally, faced with drained public accounts and a mandate for change, states that have suffered generations of corruption may not be in a position to dedicate significant resources to the pursuit of lost value, a process that can be extremely complex and far reaching, typically involving the movement of proceeds of crime to multiple jurisdictions around the globe.

[20] Channels Television (2020) Nigerian Govt Receives $311m Abacha Assets From US, Jersey, available at: https://www.channelstv.com/2020/05/04/nigerian-govt-receives-311m-recovered-abacha-assets-from-us-jersey/

Complex problems call for complex solutions and there are professional services firms of investigators, lawyers, and forensic accountants specialising in the recovery of the proceeds of fraud and corruption. In response to the question of funding over the past decade or more, there has also been a growing cadre of private funding firms that can assist governments in a range of funding alternatives. Deciding on whether to engage a private funder can be a challenge given the risk associated with civil asset recovery, as there is with any litigation. These types of funding arrangements necessarily demand a commensurate return on investment. Once again, presentation with full transparency to the public is critical to obtain public buy-in from a political standpoint. When the decision is whether to proceed or not, a case can often be made to satisfy the cost-benefit analysis of giving up part of something, or all of nothing. Experience has shown that investing state resources at the outset can accomplish several key benefits that can jumpstart a successful civil asset recovery strategy:

- First, self-funded preliminary investigations can help develop leads to potential asset recovery that can lead to early identification of actionable wrongdoing and possible targets for recovery. Actionable intelligence is extremely important and attractive to private funders and legal counsel who will be engaged to develop and bring claims.

- Positive preliminary findings can also reduce the risk to private funders who will not be asked to put capital at risk at an exploratory stage. Lower risk results in a lower premium required on the funder's investment, translating to overall reduced cost, which means higher net recovery to the state.

- Finally, preliminary targeted investigations can serve as harbingers of things to come if a full-scale corruption investigation and asset recovery case is commenced. They serve as trial run that can identify weaknesses in chain of command, assess the existence and quality of access to information, and they can test the political will and leadership of those in government who are directing the recovery.

The Civil Asset Recovery Strategy

The civil asset recovery strategy encompasses specialist professional service providers that span several competencies, with each one having a degree of knowledge and experience commensurate with each other. The most successful recovery cases are comprised of professionals who collaborate well, each bringing multi-jurisdictional experience and skill to their respective fields. While the involvement of each element of the team of recovery professionals will vary at different times, it is important for all to be aware of the status of the case and the direction that it is taking. A well-informed team will keep a civil asset recovery case focused on realistic claims for value, alert to potential challenges, and aware of potential parallel criminal proceedings to the extent they help and do not hinder the civil recovery. The civil asset recovery strategy typically includes multiple rounds of data preservation, investigative interviews and intelligence gathering, the formulation of legal claims, and the implementation enforcement strategies.

Data Preservation

Information and data preservation is one of the most critical first steps that will establish a critical foundation upon which entire investigations and consequent asset recovery cases may succeed or fail. This step is often carried out at a very early stage when very little may be known about the complete nature of the wrongdoing or the scope of the participants, both within and outside the government. Significant attention must be given to consider the possible universe of data that may be required. Once the preservation process is commenced, the risk of destruction of documents and devices grows exponentially, and careful consideration should be taken to cast the net as wide as possible. Data preservation includes many different sources of information. An ever-changing set of skills and technology is required to capture hard copy records, end-user devices, computer servers, and cloud-based data. Investigation and intelligence professionals interrogate the information that drives the recovery case.

Investigation and Intelligence Gathering

An early assessment of electronic data can range from financial databases, email servers, text messaging and other forms of communications, social media, official contracts, procurement information, and related policies and regulations. Armed with this, investigators and intelligence professionals begin to build the foundations of the case.

Information gathering also involves conducting interviews with functionaries and senior officials alike, as well as reports from whistle blowers, data analysis, and search strings run across millions of records. These help to pinpoint areas of concern. Individual contracts or entire departments come under scrutiny and key individuals are identified. Investigation and intelligence gathering can be an iterative process, distilling findings into actionable evidence and informing possible legal claims.

The investigative team work closely with legal advisors, providing reports and analyses that ultimately frame claims for recovery of value, which take on a variety of forms. These include the cars, homes, and yachts previously mentioned as more traditional hard assets, but assets often take a softer form including claims for value lost because of actions or inaction by a service provider. Communications between government officials, their advisors, and colluding parties in the private sector may set the stage for third party claims.

Legal Claims and Subject Matter Experts

Legal claims range from graft by single contractors providing bribes in return for the award of multi-million dollar contracts, which are easy to quantify, to claims for economic harm brought to an entire state due to cartel behaviour by oligarchs controlling an entire industry.

Legal professionals draw on the financial analyses completed by investigators which may show trends in contract award values that are indicative of collusive activity. These hallmarks must then be substantiated by subject matter experts who test things like the integrity of roads and bridges to ensure they meet the technical specifications contracted for by the government. The legal and investigative teams collaborate to leverage findings to support applications for production of bank

records, phone records, and information about properties, companies, and trust structures in domestic and foreign jurisdictions. This serves to develop increased knowledge in order to support the investigative and legal hypothesis, leading to claims.

As successful claims are brought, the resulting awards are taken to foreign jurisdictions when assets have moved, to be recognized for enforcement abroad. In order to synchronise the legal outcomes from one jurisdiction to another, a well organised network of investigative and legal professionals practicing in the niche field of cross-border asset recovery is required.

Grand corruption cases often involve multiple claims against multiple parties. These claims are often segregated by the type of action or by classes of individual, corporate, or trusts which are the subjects of the claims. Rarely do the chronologies of the varied actions align, which means judgments can be issued at different times in various amounts and may involve different strategies for enforcement.

Asset Recovery and Enforcement Through Insolvency

An often-overlooked tool for enforcing judgments against individuals and corporate entities is the use of insolvency proceedings, which can be advantageous to gaining access to physical or financial assets in domestic and foreign jurisdictions. Equally, or more often, there can be value in using insolvency laws to gain access to banking records or any other information that a company holds. Stepping into the shoes of a shelf company in an offshore jurisdiction can be a low-cost, time effective approach to gaining access to records that might otherwise be unavailable or could be complicated by an official government-to-government diplomatic channel or through law enforcement. The use of information gained through government or criminal procedures may be problematic or even impossible to use in a civil proceeding. The civil asset recovery team must be alert to these and other potential pitfalls.

Final Considerations

Combatting political corruption, by its nature, presents many threats and sensitivities to all involved. While the objectives of governments, their advisors and funders, and the general public may align at the outset of a civil asset recovery case, the relationships can easily fray when political demands become paramount, timelines for investigation or legal claims inevitably run longer than anticipated, or, when financial investments deviate from the plan. Professional advisors must carefully assess the moral and financial risks associated with acting for regimes in charge. Independence must be maintained, and legal and financial advisors need to be wary of political motivations and ensure preliminary findings are not misconstrued for political theatre. Similarly, findings that go deeper than anticipated may be whitewashed or never see the light of day.

Funders, and therefore, the team of professional advisors, rely on good faith that the government will allow claims to be fully developed and recoveries to be made to secure their own compensation. Findings that threaten the current apparatus may pose an existential threat to the investigation and asset recovery plan, and can cause severe financial harm to professional advisors. As such, they should ensure that sufficient contingencies are built into the contract terms.

To provide the optimal setting for successful asset recovery to governments, the most important factors must include empowerment from the top, access to people and information, and a clear operational strategy rather than a politically motivated one. Only once these guiding principles are in place will there be an opportunity to help recover lost value into the government treasury and to help a nation stand up to corruption.

About the Author

James Pomeroy is a Director in Grant Thornton's Forensic practice and has 25 years of insolvency, audit, forensic accounting, and investigations experience. He is a Chartered Professional Accountant, a Fellow of INSOL, and a Certified Forensic Accountant and leads Grant Thornton's Forensics practice in the BVI and Cayman Islands. James' experience includes cross border insolvencies, international asset tracing investigations, investigations of political corruption, the offshore financial sector, business intelligence and integrity due diligence, commercial disputes, forensic technology cases, and asset recovery. He has extensive experience in jurisdictions throughout the Caribbean region, Latin America, Canada, the US, and Hong Kong. James has led insolvency-based asset tracing and recovery engagements into multiple jurisdictions worldwide, often involving the application of *ex parte* discovery orders. James is an experienced insolvency and forensic professional with an appreciation for the nuances of different regions and cultures and how those can impact a case. He is a regular presenter on the topics of cross border insolvency-related fraud and asset recovery.

James Pomeroy
Director, Forensic
Grant Thornton BVI Ltd
PO Box 4259 | 171 Main Street | The Barracks | Road Town | Tortola | British Virgin Islands
T +1 902 452 1755
E. James.A.Pomeroy@uk.gt.com W. grantthornton.vg

Grant Thornton

Developments in Asset Tracing: A Cayman Islands Perspective

Nick Dunne &
Colette Wilkins

Abstract

In this article, Nick Dunne and Colette Wilkins, partners at the law firm Walkers, based in the Cayman Islands, share their insights on recent developments in asset tracing, by reference to locally-decided cases with international relevance. The authors provide important backdrop to the offshore world set against growing transparency initiatives and increased scrutiny at government and inter-governmental level.

The Compliance Dividend

The traditional image of the offshore jurisdictions as a regulatory black hole into which money disappears but information never comes out is powerful and enduring, but also increasingly inaccurate. Regardless of beaches and palm trees, no jurisdiction is truly an island, and offshore centres are now better understood as the busy intersections of international financial business.

A natural consequence of that place in the global system is that growing regulatory burdens in the onshore world have been reflected offshore, a harmonisation that is necessary to ensure continued cooperation and access to that global system. Not only have the (in)famous provisions of the old Confidential Relationships (Preservation) Law been fundamentally overhauled to remove the features which were often characterised as a "secrecy law" , but regular inspections by the Financial Action Task Force of the Organisation for Economic Cooperation and Development have resulted in what amount to mandatory risk mitigation recommendations. The attention of numerous national and intergovernmental agencies has also been directed to addressing perceived abuses of the tax system, with the result that the Islands find themselves under constant and detailed scrutiny. In consequence, secrecy and concealment have increasingly given way to transparency and tax efficiency as the hallmarks of the mature offshore world, with a corresponding eagerness to avoid any association with "dirty" money.

A welcome by-product of that shift of emphasis has been to assist in asset recovery efforts in a number of ways. The first of which relates to the usefulness of the existing Norwich Pharmacal remedy. As is well known, such enables disclosure to be obtained from an innocent non-party where that information is necessary to identify a wrongdoer or bring a claim. Norwich Pharmacal orders have always been a powerful weapon when deployed against offshore service providers such as registered agents or banks, but the increasing need for collection and updating of detailed due diligence can result in a wealth of useful information being identified where a fraudster may have utilised a Cayman Islands vehicle beyond that which may have previously been available.

In similar vein, the identity of the directors of an entity is often a matter of significant interest, but for many years was out of reach without the need to first obtain a Norwich Pharmacal order, because the register was a confidential document which, although filed with the Registrar of Companies, was not open to public inspection. That has however recently changed, and a list of current directors may now be obtained directly from the Registry upon payment of a small fee. Although this will not always avoid the need to obtain wider disclosure, its immediate availability and low cost can be important and helpful, particularly where a matter is developing quickly. The usefulness of this data is of course entirely contingent upon its accuracy, but initial signs in that regard are encouraging.

The introduction of economic substance requirements for many Cayman Islands companies as part of regulatory reform has marked a departure from the "brass plate" model of business, where the fact of a company registration was rarely linked to a physical presence within the Islands, to a situation in which an more tangible existence will be far more common. Although there are a number of exemptions to the rules, most companies are now required to maintain an "adequate physical presence" in the jurisdiction when assessed in relation to the level of income that they generate, which in many cases will require both a place of business and local staff.

That is another change which may affect the asset recovery landscape given that a physical presence is likely to lead to a commensurate expansion in the quantity of potentially relevant documentation within the Islands, and the presence of individuals who may be involved in any wrongdoing. Given the pro-recovery attitude of the Cayman Islands courts and the range of remedies available to assist in recovery and tracing, connection with the Cayman Islands may well prove a vulnerability, rather than a strength, for fraudsters.

Perhaps most importantly of all, the overarching narrative of the past 15 years in the Cayman Islands has been firmly one of a move to a pro-compliance business culture which is aligned with that which exists in the larger onshore jurisdictions. Whilst it would be naïve to either conclude that fraud has been eliminated, or that there are not jurisdictions in which the old ways do not still hold sway, the chilling effect of that positive culture on the opportunities which might otherwise exist for fraud should not be underestimated. The contradiction is, perhaps, that as the ways in which to commit fraud increase with the rise of technology, so the ways in which to safely warehouse the proceeds of those frauds decline. Fraud may be an inevitability, but the Cayman Islands has firmly sought to align itself with the victim in seeking to unravel wrongdoing.

Hands Across the Sea

Notwithstanding the developments in relation to economic substance, it nevertheless remains the case that the vast majority of businesses connected with the Cayman Islands have an overwhelmingly strong international element. It is a rare fraud claim indeed which starts and finishes in the offshore world without travelling onshore at some stage. Against this background, the effectiveness of asset recovery measures is heavily dependent on the extent to which they are able to successfully interact with proceedings in other jurisdictions which may have a substantially greater connection to the fraud itself, and may well be the situs of any substantive claims against the fraudster.

The Cayman Islands has been proactive in that regard, most obviously through a successful amendment to the Grand Court Law which placed it beyond doubt that jurisdiction existed to grant injunctions ancillary to overseas proceedings even where there was no cause of action within the Islands. Orders freezing assets under those provisions are now made frequently.

The statutory basis for these freestanding orders has avoided the difficulties which have recently arisen in the British Virgin Islands with the "Black Swan" line of cases beginning in 2009. Such sought to achieve at common law the same effect as the Cayman Island statutory amendment, and were recently held by the Eastern Caribbean Court of Appeal in *Broad Idea International v Convoy Collateral* (BVICMAP 2019/0026, 29 May 2020) to have been wrongly decided. This leaves a lacuna in the law, albeit one that that jurisdiction is likely to remedy in short order. Currently pending appeal, doubtless that hole will be plugged statutorily in due course, but the uncertainty that has resulted from *Broad Idea* both demonstrates the prescience of the Cayman Islands approach and the pro-assistance attitude of the Court to proceedings in foreign jurisdictions.

Another example of that attitude can been found in a very recent (and as yet unreported) decision of the Grand Court. This involved allegations of serious wrongdoing in respect of a locally incorporated and regulated insurer, whose business was principally conducted in the United States, but there was a potential lacuna in the law as to whether the Court was able to confirm the powers of locally appointed controllers so as to enable them to apply for urgent Chapter 15 relief and temporary restraining orders in the United States.

Recognising the importance of US bankruptcy protection to the interests of potential creditors, the Court was willing to look beyond the failure to expressly provide a power to give such a confirmation in the relevant statutes and take the view that it was able to make the necessary orders in the exercise of its inherent jurisdiction. As a result, the interim relief was secured within a matter of hours.

Although this decision was focused on a discrete and specialised point, the flexible and pragmatic approach which was adopted in the interests of securing assets is consistent with the prevailing trend over a number of years, and there is no reason to foresee any change in that trend in future. The ability of the Cayman Islands courts not only to adopt and follow trends in asset

recovery from elsewhere, but to recognise the importance of cooperation and comity in seeking to do justice in asset recovery matters, is beyond doubt and is demonstrated on a regular basis. The Grand Court has clearly signalled that it understands the nature of its role in cross border disputes, and will do all it properly can to work alongside foreign courts to ensure the effectiveness of remedies granted at home or abroad.

Concluding Thoughts

Any notion of the major offshore jurisdictions as sleepy backwaters has been firmly dispelled by in recent years. Dynamic change is underway, both judicial and legislative a state of affairs which appears likely to continue for the foreseeable future. The direction of travel is likely to remain in favour of parties seeking to trace and recover assets, providing an increasingly powerful toolkit to practitioners.

About the Authors

Nick Dunne joined Walkers' Cayman Islands office in 2008 and is a partner in the firm's top-tier Insolvency & Dispute Resolution Group. His practice focuses on major and complex international and cross-border commercial disputes and arbitrations with a particular interest in fraud and asset recovery. Nick frequently appears before the Grand Court and the Cayman Islands Court of Appeal, and also has experience of appeals to the Judicial Committee of the Privy Council. Nick has also been listed as a recommended lawyer in the leading independent legal directories, including Chambers Global, Legal 500 and Who's Who Legal.

Colette Wilkins has been a commercial litigator for 30 years, specialising in contentious insolvency, high value asset recovery, investment fund disputes and issues relating to corporate governance and fraud. She advises office-holders in complex cross-border liquidations, and regularly represents creditors and liquidators in insolvency and related proceedings to determine and protect interests in insolvent estates. Colette advises and appears for clients on issues relating to corporate governance and fraud as well as other areas of commercial litigation. She has been a partner in the Insolvency and Dispute Resolution Group since 2009 and since then has been commended in all the leading independent legal directories including Chambers Global (Band 1), Legal 500 (Tier 1) and Who's Who Legal (Thought Leader). Colette addresses issues relating to Cayman Islands asset recovery and insolvency at conferences on a regular basis and was a speaker at the United Nations Commission on International Trade Law Colloquium on Civil Asset Tracing and Recovery in Vienna in December 2019. She is also one of the two attorneys appointed by the Chief Justice to sit on the Cayman Islands Grand Court Rules Committee.

Nick Dunne
Partner, Walkers

T. +1 345 814 4548
E. nick.dunne@walkersglobal.com

Colette Wilkins
Partner, Walkers

T. +1 345 914 4215
E. colette.wilkins@walkersglobal.com

WALKERS

Exceptional Means to Assist With Multi-Jurisdictional Asset Tracing and Recovery in Panama

David M. Mizrachi

Abstract

This article explores direct means of obtaining evidence and provisional measures in aid of foreign proceedings under the laws of the Republic of Panama, which are available in lieu of traditional means of international judicial assistance such as letters rogatory and enforcement proceedings.

1. Introduction

Litigants embroiled in international civil and/or commercial disputes requiring the tracing or recovery of assets in more than one jurisdiction, are frequently faced with challenges due to differences in the legal systems of such jurisdictions. Of particular relevance is the marked lack of compatibility between Common Law and Civil Law jurisdictions. The concepts of comity and reciprocity are not always fully understood in the same way across the different legal traditions. Thus, obtaining relief in a foreign jurisdiction can often be a very difficult endeavor. Not only are there legal, language and cultural barriers but also systemic issues which are related to bureaucratic procedures and longstanding traditions of the various jurisdictions.

Until the last decade, Panamanian legal procedures made it rather impractical for anyone seeking to enforce foreign orders in Panama. For starters, Panamanian courts are generally barred from providing judicial assistance in civil matters beyond taking evidence and serving notice of proceedings. This limitation is clear in the language of articles 99 and 100 of Panama's Code of Private International Law (2015) (the 'PIL Code').

Article 99 of the PIL Code lays out the principle behind judicial cooperation in civil matters. It states that Panamanian courts will cooperate with foreign tribunals based upon existing treaties and conventions, and, in their absence, *"by virtue of international comity [lit. courtesy] or by way of controlled reciprocity"*. Article 100 of the PIL Code clearly indicates that judicial cooperation of Panamanian courts will only be available when dealing with notifications, summons, serving process and taking of evidence. It does not mention enforcement of interim measures.

Enforcement of interim measures is also excluded from the norm dealing with enforcement of judgments, namely article 155 of the PIL Code. Said provision limits the enforcement powers of the Panamanian judiciary in civil matters to *"judgments rendered by foreign tribunals which have a res judicata effect…"*. Even prior to the enactment of the PIL Code, the Fourth Chamber of the Supreme Court of Panama (in charge of judicial cooperation) was generally reluctant to grant provisional orders of relief, including the freezing of assets, or recognizing a foreign receiver, in support of foreign procedures. In that regard, *In re: Request by the Sixth Labor Court of Cartagena, Colombia*, Supreme Court of Panama, Fourth Chamber (January 28, 2004) Pereira Burgos, Justice, the Fourth Chamber has stated:

It is noted that what has been requested by the Colombian authorities, is not found within the actions previewed by the cited convention, as the annotation of the provisional measure of an embargo decreed by the Sixth Labor Court of Cartagena against the Panamanian flag Vessel…thus the Chamber may not grant what was requested by the Colombian state.[1]

Furthermore, in the case of *In re: Request by the United States of Mexico*, Supreme Court of Panama, Fourth Chamber (28 February, 2005) Spadafora, Justice, the Fourth Chamber of the Supreme Court of Panama held:

"The Fourth Chamber of the Supreme Court of Justice has repeatedly stated that the securing of assets for our laws is a provisional measure, which cannot be considered a merely procedural action.[2]

Finally, *In re: Narfason*, Supreme Court of Panama, Fourth Chamber (9 February 2015) Mitchell, Justice, the Fourth Chamber stated:

"…that the foreign ruling which enforcement in our country is sought, is a jurisdictional act of a formal and declarative nature, which does not issue a ruling over the substance of the legal situation posted, which is a ruling over the claim, a situation which is not identified with the authority of res judicata…"

"For that motivation, being that the condition of res judicata is an essential element for the enforcement of a judgment in our country, the ruling which enforcement is sought is missing that element, particularly since article 1419 of the Judicial Code states that 'it is understood as a judgment the decision which decides a claim", which must be final and duly served and which accordingly may not be subject to recourse, by reason of which the ruling naming the entity ERNST & YOUNG as judicial administrator or receiver of the present and future estate of its debtor 1252064 ALBERTA Ltd. may not be enforced or recognized". [3]

---

[1] In re: Request by the Sixth Labor Court of Cartagena, Colombia, Supreme Court of Panama, Fourth Chamber (January 28, 2004) Pereira Burgos, Justice. http://bd.organojudicial.gob.pa/rjhtml/generales/rj200401-0000-4-15-71-10-$74-03$-$8-81-81$-20040128-M.htm

[2] In re: Request by the United States of Mexico Supreme Court of Panama, Fourth Chamber (28 February, 2005) Spadafora, Justice. http://bd.organojudicial.gob.pa/rjhtml/generales/rj200502-0000-4-15-72-10-$824-04$-$7-58-878$-20050228-M.htm

[3] In re: Narfason, Supreme Court of Panama, Fourth Chamber (9 February 2015) Mitchell, Justice. http://bd.organojudicial.gob.pa/scripts/dtSearch/dtisapi6.dll?cmd=getdoc&DocId=2229&Index=H%3a%5cdtsearch%5cUserData%5cindices%5fdts%5ccorte%5cgenerales&HitCount=7&hits=34+86+140+24a+3c9+4f4+596+&SearchForm=c%3a%5cinetpub%5cwwwroot%5cregistro%5fform%2ehtml

2. Exceptional Means of Judicial Cooperation

While the general rule seems to limit the tools available by way of judicial cooperation, there are three instances which allow direct cooperation without the need to resort to the cumbersome and formality-ridden letter rogatory or *exequatur* procedures.

Prior to the enactment of the PIL Code, there were only two exceptions to the rule. The first was when dealing with foreign estate proceedings and the second when dealing with provisional measures in the context of a foreign arbitration proceeding. The third exception came with the advent of the Insolvency Law (2016), which became effective in 2017.

3. Enforcement and Judicial Assistance in Foreign Estate Proceedings

With regards to foreign estate or probate proceedings, article 1523 of Panama's Judicial Code states:

1523. *When the order naming heirs or the resolution adjudicating* ***has been issued by a foreign Tribunal,*** *and the deceased has left assets in the country, the edicts shall be fixed and published and* ***the procedure established in articles 1510 and subsequent shall be followed****.* (emphasis added).

This provision obviates the need for the foreign court or the representative of the estate to follow the letter rogatory or the *exequatur* rules found in the PIL Code. In fact, there are several Supreme Court (Fourth Chamber) cases denying enforcement and remitting the applicants to this norm.

4. Cautionary Measures in Foreign Arbitral Matters

Panama's Arbitration Law (2013) also provides litigants with useful tools to assist arbitration proceedings taking place abroad. Article 44 of the Arbitration Law states:

Article 44. *Jurisdiction of the judicial tribunals. The judicial tribunal shall have* ***the same jurisdiction to issue cautionary measures*** *in the service of arbitration acts* ***independently of whether these be substantiated or not in the country of its jurisdiction,*** *as it has in the service of judicial actions. The judicial tribunal shall exercise said jurisdiction in conformity with its own procedures and* ***taking into account the distinctive traits of international arbitration****.* (emphasis added).

Under this provision, a Panamanian court has jurisdiction to issue provisional measures in aid of foreign arbitration proceedings. Thus, it is clear that under the circumstances, there is no requirement that the arbitration panel make a request to the Panamanian Courts. The parties can request the assistance directly. It is important to note that the Supreme Court of Panama, in the case of *Greenhow adv. Refinería Panamá*, Supreme Court of Panama, Fourth Chamber (14 February, 2005), Spadafora, Justice has compared arbitrators to judges and has stated:

"Accordingly, ***arbitrators are turned into judges at law*** *and their decisions have coercive force in front of the rest of the judicial and administrative community, giving the parties increased security that their claims, recognized in the arbitral awards shall be respected".* (emphasis added)[4]

The Arbitration Law grants foreign arbitration panels the same status when it allows local courts of law to cooperate with arbitration proceedings taking place abroad.

5. International Insolvency

In 2016 Panama enacted its Insolvency Law, which came into force in 2017. The Insolvency Law included several provisions which facilitate communications and cooperation between insolvency courts or insolvency agencies in foreign countries and the insolvency courts of Panama. Assets belonging to companies incorporated or doing business in Panama which are part of a foreign insolvency may be pursued in Panama with the aid of the Panamanian courts, without the need to file letters rogatory.

According to article 210, these provisions were enacted in order to encourage cooperation between Panama and foreign jurisdictions, to advance the rule of law in business and investments, to efficiently manage transnational insolvencies to protect the debtor's assets and to optimize their value, and to reorganize companies in financial difficulty.

The Insolvency Law allows a foreign court or representative to request assistance from the Republic of Panama in relation to foreign proceedings. Under this legislation, a Panamanian court may request assistance from foreign jurisdictions and it allows for the simultaneous execution of insolvency proceedings in Panama and abroad. The Insolvency Law provides foreign creditors with very useful tools such as expedited evidence gathering and the right to freeze assets without having to post a bond, even in cases where the main insolvency proceeding is taking place outside of Panama. Again, there is no need to resort to letters rogatory or *exequatur* proceedings.

6. Conclusion

Breaking traditional judicial practices is a very cumbersome and long process, particularly along different judicial systems. The Panamanian judicial system is no exception, especially when dealing with Common Law or non-Spanish speaking jurisdictions. Nevertheless, within the context of civil and commercial disputes, Panama has been assuming a more cooperative position with regards to its foreign peers. In fact, in fiscal and criminal matters, the cooperation is even more open and forthcoming. With the enactment of the Arbitration Law, it became clear that the country's judiciary was going to be more cooperative to its foreign peers.

As we have discussed, just a short five years ago, the Supreme Court refused to recognize a foreign insolvency receiver on grounds that the recognition did not involve a final judgment on the merits. Now, foreign insolvency representatives are allowed to directly seek the assistance of

[4] Re: Greenhow adv. Refinería Panamá, Supreme Court of Panama, Fourth Chamber (14 February, 2005), Spadafora, Justice.
http://bd.organojudicial.gob.pa/scripts/dtSearch/dtisapi6.dll?cmd=getdoc&DocId=34869&Index=H%3a%5cdtsearch%5cUserData%5cindices%5fdts%5ctodo&HitCount=36&hits=2b+67+c8+e2+118+12f+1c0+207+21d+27b+2cb+2da+30f+390+3f1+426+502+56a+5ef+875+a72+abc+af9+104b+1061+1075+10a7+10bd+1126+1176+1185+11ba+16a4+16b2+17e0+184f+&SearchForm=c%3a%5cinetpub%5cwwwroot%5cregistro%5fform%2ehtml

Panamanian courts in insolvency matters taking place abroad. Our recent experience in these three areas of the law (estates, arbitration and insolvency) has been positive in the sense that the lower courts in Panama have been, to the most extent, cooperative with the foreign courts involved.

To the extent Panamanian courts are more open to assist foreign litigants, it is likely that foreign courts will follow suit when Panama-based litigants are trying to pursue assets or evidence located abroad. It is incumbent upon the many governments to find ways to facilitate judicial cooperation, particularly in matters involving lost or absconded patrimonies. These situations require swift assistance and minimal red tape in order to be effective and efficient. Modern, forward-looking legislation like the ones we have examined in this paper are a good way to achieve those goals.

About the Author

David M. Mizrachi is the founding partner of MDU Legal in the Republic of Panama. He received a BA (Hons) in Political Science and Economics from the University of Pennsylvania and a Juris Doctor degree *cum laude* from Tulane Law School, and is admitted to practice in Panama and the State of Florida. He lectures in International Law at Quality Leadership University and is an Authorized Public Translator (English-Spanish-English). Much of David's international practice focuses on asset-tracing and recovery, cross-border insolvency and complex commercial litigation. He recently obtained the first recognition of a foreign insolvency based upon Panama's new Insolvency Law. Other examples of recent work include obtaining an *ex parte* suspension order halting the exercise of corporate rights by a shareholder holding bearer shares in a corporation; and the pre-filing appointment of a judicial administrator of a company suspected of defrauding investors. He routinely assists foreign firms and governmental agencies with legal needs in Panama and coordinates multinational litigation efforts for local clients. He has served as an expert on Panamanian law in cases in New York, Florida, Indiana, Washington State, Bermuda, Israel, Jersey and the UK, and has spoken internationally on legal matters including asset-tracing and recovery. David has been named one of the world's *Thought Leaders* ('Global Elite') for Asset Recovery (*Who's Who Legal*, Asset Recovery 2020) and is listed as an Expert in Litigation, Corporate Law and Arbitration. His firm was chosen the Firm of the Year in Panama in the WWL Awards (New York, 2016). He and his firm are ranked by Chambers and Partners (Latin America 2021) in the areas of Dispute Resolution and Corporate/M&A, and featured in Chambers Global (2021). David is the Panamanian member of ICC FraudNet and Trace International. He is author of the Panama Section of the FraudNet Compendium on Asset Tracing and Recovery (Eric Schmidt Verlag, 2010), Digest of the Commercial Laws of the World (Thomson Reuters 2018) and a contributor to World Bank's Asset Recovery Handbook (Brun, et. al 2011).

David M. Mizrachi
Founding Partner, MDU Legal

T. +507-263-0604
E. david@mdulegal.com
W. linkedin.com/in/davidmdulegal

MDU LEGAL

Does Ghana's Legal Regime for Tracing and Recovering Assets Procured by Cross-Border Fraud Offer Enough Protection for Foreign Victims?

Bobby Banson

Abstract

In this article, Bobby Banson of the Robert Smith Law Group, Ghana examines the existing legal regime in Ghana relating to protections for victims of cross-border fraud by reference to recent legal developments and decided cases in the jurisdiction. His analysis builds upon his earlier published work 'Tracing and Recovering Assets in Ghana: Has Ghana's Supreme Court laid down a New Standard?'

Introduction[1]

One of the most common crimes reported in Ghana's media is fraud. Internationally, there have been several reports of foreign nations who have allegedly been victims of internet scams and other offences involving dishonest conduct emanating from Ghana. The Ghana Police Service has since set up a special unit to deal with cybercrime and related fraudulent activities. It goes without saying that millions of dollars are lost by victims through such fraudulent activities. In this article, I discuss the existing legal regime in Ghana which seeks to protect victims of such fraudulent activities. In doing so, the provisions of the Criminal Offence Act, 1960 (Act 29) Companies Act, 2019 (Act 992) case law as well as the applicable common law provisions which are deemed to be part of the laws of Ghana by virtue of the provisions of the 1992 Constitution, will be discussed.

1. Jurisdictions of Ghanaian Courts in Cross-Border Fraudulent Transactions

Broadly, the jurisdiction of the Ghanaian Courts can be invoked in both criminal and civil actions. For Civil actions, the 1992 Constitution provides that the High Court of Ghana has original jurisdiction in all matters. For a foreigner to be able to institute a civil action in Ghana to recover assets that he has lost due to fraudulent activities, the perpetrator of the fraud must be resident in

[1] See: Banson 'Tracing and Recovering Assets in Ghana: Has Ghana's Supreme Court laid down a New Standard?' at: https://ghanalawhub.com/tracing-and-recovery-of-assets-in-ghana-has-ghanas-supreme-court-laid-down-a-new-standard/, published on April 25, 2020.

Ghana or the purported contract ought to have been executed in Ghana. For Criminal actions, Section 56 of the Courts Act, 1993 (Act 459) confers jurisdiction on the Ghanaian Courts in criminal matters where the offence is committed by a Citizen of Ghana or by a person who is resident in Ghana if the offence if wholly or partly committed in Ghana.

2. Cause of Action for Victims

Under Ghanaian, Law, victims of dishonest conduct could decide to proceed with a criminal prosecution or commence civil action. Both actions could be commenced simultaneously. However, a Judge exercising criminal jurisdiction cannot make orders which will only be available if a civil action had been commenced. This article proceeds to look at the remedies available for a victim who initiates criminal proceedings and the remedies available for a victim who initiates civil proceedings.

3. Criminal Prosecution

A victim of a cross border dishonest conduct can initial criminal proceedings in Ghana by lodging a complaint with the Ghana Police Service, which operates under the Office of the Attorney General of the Republic of Ghana. All criminal prosecutions are initiated by a State Prosecutor after a complaint is lodged by a victim.

3.1 Criminal Offences Involving Dishonesty Under Ghanaian Law

In Ghana, the Criminal Offences Act is the law which principally regulates actions or inactions which are punishable by a fine, imprisonment or death. However, other laws also provide for criminal actions for certain actions or inactions. Chapter 1 of the Criminal Offences Act provides for offences involving dishonesty such as stealing, dishonest breach of trust, dishonest appropriation and defrauding by false pretences. Each of these elements will be briefly explained to contextualise the types of offences which this paper concerns to determine whether which assets procured therefrom are recoverable under Ghanaian law.

a. Dishonest Appropriation

Section 120 of the Act defines dishonest appropriation as:

"An appropriation of a thing is dishonest if it is made with an intent to defraud or if it is made by a person without claim of right, and with a knowledge or belief that the appropriation is without the consent of some person for whom he is trustee or who is owner of the thing, as the case may be, or that the appropriation would, if known to any such person, be without his consent."

b. Stealing

As per the provisions of Section 125 of the Act:

"a person steals if he dishonestly appropriates a thing of which he is not the owner."

c. Defrauding by False Pretences:

Section 132 of the Act provides that:

"A person is guilty of defrauding by false pretences if, by means of any false pretence, or by personation he obtains the consent of another person to part with or transfer the ownership of anything."

Section 133 further provides:

(1) A false pretence is a representation of the existence of a state of facts made by a person, either with the knowledge that such representation is false or without the belief that it is true, and made with an intent to defraud.

(2) For the purpose of this section—

(a) a representation may be made either by written or spoken words, or by personation, or by any other conduct, sign, or means of whatsoever kind;

(b) the expression "a representation of the existence of a state of facts" includes a representation as to the non-existence of any thing or condition of things, and a representation of any right, liability, authority, ability, dignity or ground of credit or confidence as resulting from any alleged past facts or state of facts, but does not include a mere representation of any intention or state of mind in the persons making the representation, nor any mere representation or promise that anything will happen or be done, or is likely to happen or be done;

(c) a consent shall not be deemed to have been obtained by a false representation as to the quality or value of a thing, unless, the thing is substantially worthless for the purpose for which it is represented to be fit, or to have been substantially a different thing from that which it is represented to be; and

(d) subject to the foregoing rules, if the consent of a person is in fact obtained by a false pretence, it is immaterial that the pretence is such as would have had no effect on the mind of a person using ordinary care and judgment."

4.2 Remedies Available to Victims of Dishonesty Offences Under Ghanaian Law

Under Ghanaian Law, where criminal proceedings are concluded and the alleged perpetrator of a criminal offence involving dishonesty is found guilty, the law provides a remedy to the victim of the offence. Section 146 of the Criminal and Other Offences (Procedure) Act, 1960 (Act 30) provides:

"Where any person is convicted of having stolen or having obtained any property fraudulently or by false pretences, the Court convicting him may order that the property or a part thereof be restored to the person who appears to it to be entitled thereto".

5. Civil Action

Even though fraud connotes a criminal offence, it could also be the basis of a civil action. Where a victim alleges that he has lost property due to fraudulent misrepresentation or dishonest conduct, the victim may commence a civil action for relief to enable the victim to be put in the same position that the victim was in before the dishonest conduct occurred.

5.1. Relationship of Trust

Where there is a relationship between the parties, fiduciary or not, the victim could institute civil proceedings under the common law of trust. Where there is a breach of a trust agreement, the assets could be easily traced and recovered for the benefit of the settlor or the beneficiary of the trustee. Three types of trust have been identified as applicable in Ghana. These are express trusts, resulting

trusts and constructive trusts. In the case of *Doe v Opoku-Ansah* [1997-1998] 2 GLR 149,[2] Aikins JSC, held, in respect of resulting and constructive trusts:

"A resulting, implied or constructive trust is created by a transaction between the trustee and the cestui que trust in connection with the acquisition by the trustee of a legal estate in land, whenever the trustee has so conducted himself so that it will be inequitable to allow him to deny to the cestui que trust the beneficial interest in the land acquired. And he will be held so to have conducted himself if by his words or conduct; he has induced the cestui que trust to act to his own detriment in the reasonable belief that by so acting, he was acquiring beneficial interest in the land." (pg. 158-159)

In his book, *Modern Principles of Equity* (1988),[3] A.K.P Kludze defines a resulting trust and a constructive trust as follows:

"A resulting trust arises where the owner of property has conveyed it to another person with the intention of creating a trust, but the beneficial interest returns or 'results' to the transferor because the trust has not exhausted the entire estate…A constructive trust arises by operation of law as distinguished from the act of the parties. It is a trust imposed by equity…when the circumstances are such that equity would consider it an abuse of confidence for the owner to hold the property for his own benefit."(p 272-273)

Where the trustee has wrongfully disposed of trust property, the beneficiary may attach and proceed against the trust property, even in a changed form, instead of maintaining only a personal action against the trustee for a breach of trust. In *Gateway Worship Centre v David Soon Boon SEO* [2010] SCGLR[44]; the Supreme Court of Ghana, stated:

"A person in a fiduciary position is not permitted to profit from his position (see *Re Biss* [1903] 2 Ch 40). The general principle, as stated in the locus classicus case of *Re Diplock's Estate* [1947] Ch 716 at pages 744-745, is that whenever there is or has been a fiduciary relationship, the beneficial owner of an equitable interest in property may trace it into the hands of anyone holding the property, except a bona fide purchaser for value without notice whose title is, as usual, inviolable. Once it is not a bona fide purchaser for value without notice who has acquired the land in dispute, the money raised in Korea for the benefit of the 2nd Respondent is traceable in equity to any hand whatsoever and in any form it, or part thereof, has been used to acquire. Therefore, whatever has been acquired by any monies that are proven to be part of the funds from Korea is deemed to be for the benefit of the church."

Where a trust relationship exists, the courts more often than not, as indicated above, show a favourable disposition towards the tracing and recovering of assets from a trustee on behalf of a beneficiary.

5.2. Where there is No Relationship of Trust

However, it is not in all cases that victims would have parted with money under false pretences. There could be situations where the victims have had no prior communication with the criminals and yet their assets have landed in the hands of these criminals. With the advancement of technology has come more sophisticated means by which people perpetrate "fraud" without having any form of direct contact with their victims. In such situations, it would be difficult to say fraud or theft has occurred though assets belonging to the victim have landed in the hands of other person. Therefore, what remedies do victims have in such circumstances?

---

[2] *Doe v Opoku-Ansah* [1997-1998] 2 GLR 149, at [158-159].
[3] Kludze, A.K.P (1988) *Modern Principles of Equity* (Reprinted in 2014), Walter de Gruyter GmbH & Company.
[4] *Gateway Worship Centre v David Soon Boon SEO* [2010] SCGLR.

The above scenario was the situation which befell Ecobank Nigeria in the case reported as *Ecobank Nigeria v Hiss Hands Housing Agency & Access Bank* [2019] 1 GLT 327[5]. The facts of the case were that the Plaintiff, which is based in Nigeria, had wrongly transferred an amount of $6 million into an account belonging to the Defendant, which is based in Ghana. After unsuccessful attempts to get the Defendant to refund the money, the Plaintiff issued an action for an order for the Defendants to refund the money.
The Supreme Court held as follows:

"In the case before us, although we have not made a finding of theft of the money that belongs to the plaintiff but in the 1st defendant's account by virtue of a fraud, it is right and proper that we accede to the order of restitution contained in reliefs 5 and 6 of the writ of summons herein for the following reasons. The 1st defendant has received an enrichment which came from the plaintiff and there is from the evidence no reason in law for the 1st defendant to keep that enrichment. The effect is that the 1st defendant has been unjustly enriched from funds that came from the plaintiff. The conduct of the 1st defendant in keeping the money in the face of the evidence that it came to him fraudulently from the plaintiff's account is to say the least unconscionable. Fraud and theft, in our view stand on the same footing being in their nature dishonourable acts that are perpetrated against the property of others and so we see no reason in principle that can justify a refusal of the restitutionary orders sought from the court. To withhold from the true owner the orders of restitution which are sought in the action herein, would in the circumstances of this case amount to fraud, a conduct which we desire not to condone else we would be undermining public confidence in the administration of justice. The 1st defendant from the undisputed evidence before us in these proceedings became indebted to the plaintiff to the extent of the amount transferred into his accounts held with the 2nd defendant bank. Quality justice, we note is effective justice, which from the circumstances that have unfolded before us dictates a refund to the plaintiff of the disputed amounts".

From this decision, it is clear that there is no need for the victim to plead or prove theft or fraud. All that is required is that one person has been unjustly enriched at the detriment of another person. All that needs to be established is that the person who is unjustly enriched acted dishonourably and against good conscience. Once these conditions are met, the Court will order restitution by tracing the assets which have been lost and ordering a recovery of same.

6. Beneficial Ownership

With the passage of the new Companies Act of Ghana, 2019 (Act 992), the concept of full disclosure of the names of beneficial owners of a business has further enhanced the legal rights of victims of dishonest conduct to have the veil of incorporation lifted and the assets of beneficial owners traced and recovered for the benefit of the victims. This has become important because of the tendency of such dishonest persons to invest ill-gotten wealth in companies but do not have their names appearing on the register of members.

7. Concluding Thoughts

The legal regime in Ghana, i.e. statutes and courts, is becoming awoke to cross border fraudulent activities and is taking frantic efforts to ensure that victims of such activities are able to trace and recover their assets. If a victim of such cross border fraudulent activity chooses to pursue criminal prosecution, him or his lawyer, must either directly or through the State Prosecutors, impress on the

[5] *Ecobank Nigeria v Hiss Hands Housing Agency & Access Bank* [2019] 1 GLT 327.

judge to make restitutionary orders in addition to custodial or non-custodial sentences to ensure that the victim is out in the same situation or at least close to it, before the crime was committed.
Where a civil action is pursued by a victim of such fraud, the courts have now received explicit statutory and case law backing to invoke its jurisdiction to make the requisite orders to ensure that assets of the perpetuators of the fraud are traced with the aim of putting the victims in a position that the victims were before the torts were committed.
This is a welcoming development in Ghana's legal system and should give foreign investors more comfort when doing business in Ghana.

About the Author

Bobby Banson, *Esq. LL.B., B.L., LL.M., FCIArb.* is the Founding Partner of Robert Smith Law Group, which is a boutique law firm in Accra, Ghana. He heads the firm's practice areas focusing on Alternative Dispute Resolution, Investment Advice and Corporate Governance. He has acted as Counsel in both Domestic and International Arbitration matters. Mr Banson has provided legal services to several multinational companies doing business across the West African sub region; particularly in the area of due diligence of prospective investment opportunities. He was educated at Adisadel College and earned his Bachelor of Laws (LL.B) from Kwame Nkrumah University of Science and Technology (KNUST), Kumasi-Ghana. He earned his Professional Qualification in Law (BL) from Ghana School of Law, where he graduated first in class in the Law of Taxation. He holds an LLM in International Business Law from the University of Brussels (ULB) and a Certificate in Oil & Gas Contracting. He also has a Diploma in Financial Management. Mr Banson has attended courses at Harvard University, and the Africa International Legal Awareness (AILA) Conferences. A Fellow of the Chartered Institute of Arbitrators (FCIARB), Mr Banson has spoken at various international conferences organised by CIArb and AILA and participated extensively in SOAS University of London conferences on Arbitration in Africa. Mr Banson teaches Civil Procedure at the Ghana School of Law and is the author of several journal articles relating to areas of his practice.

Bobby Banson
Founding Partner,

Robert Smith Law Group
Unit A602, Octagon Building
Central Business District, Accra, GHANA
E: bobby@robertsmithlawgroup.com
T: +233200853533

ROBERT SMITH
LAW GROUP

Part II

Legal and Regulatory Developments in Beneficial Ownership Transparency and Economic Substance Requirements

Economic Substance and Beneficial Ownership: Legal and Regulatory Developments

Anthony Riem & Priyanka Kapoor

Abstract

In this article, Anthony Riem and Priyanka Kapoor, Partners at the London firm of PCB Litigation review recent developments relating to financial regulation and the disruption of economic crime – specifically economic substance requirements and corporate ownership transparency. These developments recognise the need for and link between increased transparency and economic substance in tackling economic crime. The developments include legislation enacted by many offshore jurisdictions and crown dependencies, in response to the European Union's Code of Conduct requirements, requiring tax resident entities to demonstrate sufficient economic substance in the relevant jurisdiction. This legislation is intended to ensure that companies (and other structures) incorporated in international financial centres have sufficient substance in either the jurisdiction where they are incorporated or tax resident, increasing transparency and thereby enabling issues of tax evasion and fraud to be addressed. Furthermore, the EU's Fifth Anti-Money Laundering Directive ('5AMLD') was implemented in the UK on 10 January 2020 and the EU's Sixth Anti-Money Laundering Directive ('6AMLD') will take effect on 3 December 2020 (though the UK has opted out, as the government considers it is already largely compliant with the Directive). These Directives recognise that the transparency of beneficial ownership is crucial in preventing economic crime. Under 5AMLD, firms must inform Companies House about any material differences between beneficial ownership information a client holds and the details on the Companies House Persons with Significant Control ('PSC') register. These directives will ensure a renewed focus by jurisdictions on ensuring that information on beneficial ownership is accurate and up-to-date, thereby deterring tax evasion and other economic crime.

Introduction

Anonymity enables many illegal activities to take place hidden from law enforcement authorities, such as tax evasion, fraud, corruption, money laundering, and financing of terrorism. The regulatory developments across the world addressing the issues of economic substance and beneficial ownership are driven by the objective to lend transparency. New steps are being introduced to ensure that companies (and other structures) incorporated in international financial

centres have sufficient 'substance' either in the jurisdiction in which they are incorporated, or another jurisdiction where they are tax resident, discouraging the use of 'brass plate' companies thereby tackling the issues of tax evasion and fraud.

The economic substance standards are a global tax policy initiative driven by the Organisation for Economic Cooperation & Development ('OECD') (in particular the OECD's Forum on Harmful Tax Practices) and by the European Union's Code of Conduct Group (Business Taxation) ('Code of Conduct'). The fundamental principle behind them is to avoid domicile forum shopping, such that jurisdictions that have no or only nominal corporate tax should not facilitate structures or arrangements resulting in profits which do not reflect real economic activity in those jurisdictions. In other words, if an entity is able to benefit from low or no corporate tax by being incorporated or registered in a jurisdiction, the activities that generate its income should be performed in that jurisdiction.

In the UK, for example, case law has determined that a company that is not incorporated in the UK is tax resident in the UK if it is 'centrally managed and controlled' in the UK. The test applies to identify where the highest level of management and control over a company's affairs is exercised (i.e. where the key strategic business decisions are made), as opposed to decisions over normal day-to-day operational matters.

Transparency of beneficial ownership information is equally essential to deterring, detecting and disrupting tax evasion and other financial crimes. Beneficial owners are typically natural persons who ultimately own or control a legal entity or arrangement, such as a company, a trust or a foundation. This ownership or control can be exercised in a variety of ways, for example holding a controlling ownership interest (e.g. 25 percent or more) of a legal person. Other ways include control of a significant percentage of voting rights, or the ability to name or remove the members of an entity's board of directors. A country's domestic laws and regulations usually establish the criteria to decide the definition and scope of a beneficial owner ('BO'), with a critical consideration being that determining the BO should be independent of the BO's nationality.

Jurisdictions generally find it difficult to achieve a satisfactory level of transparency regarding beneficial ownership. Recommendation 24 (Transparency of legal persons) by the Financial Action Task Force (FATF) states that: *"Jurisdictions must ensure there is adequate, accurate and up-to-date information on basic and beneficial ownership of legal persons formed in that jurisdiction, and that such information can be provided to a competent authority in a timely manner."* For example, the UK has registers of beneficial ownership for three different types of assets: companies, properties and land, and trusts. Information on the beneficial ownership of companies is publicly available.

Legal and Regulatory Developments: Economic Substance

In response to Code of Conduct requirements, and to avoid being placed on the EU Council's list of non-cooperative jurisdictions for tax purposes (or 'blacklist') many offshore jurisdictions and Crown dependencies have enacted legislation requiring certain tax resident entities to demonstrate sufficient economic substance in the relevant jurisdiction. Each jurisdiction will have its own interpretation of an "adequate" level of economic substance, but for most it will require a company to:

(i) Carry out defined core income generating activities in that territory;

(ii) Be directed and managed in that territory: attend Board meetings in the territory and keep statutory records in the territory;

(iii) Have adequate people, premises and expenditure in that territory commensurate to the nature and scale of the relevant activity.

The table below gives a high-level overview and comparison of the economic substance laws adopted in key offshore jurisdictions:

	BVI	**Cayman Islands**	**Guernsey**	**Jersey**	**Isle of Man**	**Bermuda**
Primary Legislation	Economic Substance (Companies and Limited Partnerships) Act, 2018	International Tax Co-operation (Economic Substance) Law, 2018	Income Tax (Substance Requirements) (Implementation) Regulations, 2018, as amended	Taxation (Companies – Economic Substance) (Jersey) Law 2019	Income Tax (Substance Requirements) Order 2018 (as amended)	Economic Substance Amendment Act 2019
Sources	Economic Substance (Companies and Limited Partnerships) Act 2018.	International Tax Co-operation (Economic Substance) Law, 2018.	Income Tax (Substance Requirements) (Implementation) Regulations 2018 (as amended).	Taxation (Companies – Economic Substance) (Jersey) Law 2019.	Income Tax (Substance Requirements) Order 2018 (as amended).	Economic Substance Amendment Act 2019.
Entities in Scope	Companies incorporated or registered under the BVI Business Companies Act (excluding companies not resident in BVI) and Limited partnerships (whether local or foreign) with	Cayman companies, Cayman Limited Liability Companies (LLCs), Cayman Limited Liability Partnerships (LLPs) and Foreign companies registered in	Companies (whether incorporated under Guernsey company law, or otherwise) which: • are tax resident in Guernsey; and • receive income from a	Companies (whether incorporated under Jersey company law or otherwise) which: • are tax resident in Jersey; • conduct any Relevant Activity; and	Resident companies that derive income from a "relevant sector" (i.e, banking; insurance; shipping; fund management; financing & leasing; headquartering	All registered entities (includes companies, limited liability companies and partnerships (which have elected to have "separate legal personality") and overseas companies with a permit to engage in

	separate legal personality	the Cayman Islands	Relevant Activity whether on their own account or as a partner or member of a partnership	• receive gross income from a Relevant Activity	operation of a holding company; holding intangible property; & distribution & service centre business)	business in Bermuda)
Substance Requirements	An entity (other than a holding entity, and entities that conduct intellectual property business, for which there are different criteria) conducting a relevant activity will satisfy the economic substance requirements if: • it is managed and directed in the jurisdiction; • core income generating activities are undertaken in the jurisdiction in relation to the relevant activity; • it maintains adequate physical premises in the jurisdiction; • there are adequate employees in the jurisdiction with suitable qualifications; • there is adequate expenditure incurred in the jurisdiction in relation to the relevant activity; and • it files a confidential economic substance report each year with the applicable authority in its jurisdiction which will assist the authority in assessing compliance.					
Relevant activities	Banking • Insurance • Fund Management • Finance and Leasing • Shipping • Headquarters Activities • Distribution and Service Centre Activities • (Pure equity) holding company/entity • Intellectual property asset holding company					
Reporting	Requirement to report to BVI International Tax Authority via Beneficial Ownership Secure Search System in respect of each financial period	Requirement to make annual reports to Cayman Tax Information Authority	Prescribed information evidencing compliance to be included in annual tax returns	Prescribed information evidencing compliance to be included in annual tax returns	Prescribed information evidencing compliance to be included in annual tax returns	The Bermuda Registrar of Companies ("the Registrar") is responsible for monitoring compliance with the economic substance regime.

Legal and Regulatory developments: Beneficial ownership

Growing concerns over banking fraud, misuse of international banking systems and financial centres, and FATF recommendations, combined with increased media scrutiny following the release of the Panama Papers in 2016, have arguably led to an increase in legislative developments in this area.

Registries and public information

The 5AMLD was implemented in the UK on 10 January 2020 through the Money Laundering and Terrorist Financing (Amendment) Regulations 2019.[1] These Regulations make amendments to 'The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017' ('MLR'). Firms must inform Companies House about any material differences between beneficial ownership information a client holds and the details on the Companies House Persons with Significant Control ('PSC') register (subject to an exemption for legal professional privilege). The 5AMLD also extends the situations where ongoing customer due diligence ('CDD') must be conducted to include situations where there is a legal duty in the calendar year to contact the customer for the purpose of reviewing any relevant information relating to the beneficial owner(s).

At the EU State level, the 5AMLD introduces:

(i) wider access to each Member State's national register of beneficial ownership of corporates;
(ii) the interconnection of Member States' national beneficial ownership registers at EU level; and
(iii) the requirement for Member States to establish a central registry (or electronic data retrieval mechanism), which allows identification of natural and legal persons that hold or control bank accounts; payment accounts; or safe-deposit held by credit institutions.

The 5AMLD introduced the requirement for Registers of Trusts, where member states will have to grant public access to information held on each member state's register of trusts, subject to a "legitimate interest" test, the conditions for which must be defined in law by each individual member state. Member States must also put in place mechanisms to ensure that information on beneficial ownership in the registers of companies and trusts is "adequate, accurate and current".[2] While the trend has been towards transparency both in the UK and elsewhere, in the UK the focus has been on publicly available registers. In many jurisdictions, to the extent that there is a registry

[1] The UK Treasury launched a consultation on 15 April 2019 concerning the transposition of the 5AMLD into law and outlined how the government intended to implement the Directive. Several responses highlighted the privacy implications of collecting National Insurance or passport details and the increased risk of identity theft and fraud.
[2] The UK government has published the outcome of its technical consultation on implementation of the EU Fifth Anti-Money Laundering Directive (5AMLD) and its impact on trust registration. It has been clarified that offshore trustees entering into a business relationship in the UK will not have to register the trust on HMRC's Trust Registration Service (TRS) unless there is at least one UK-resident trustee, which was instead prescribed by the original regulation. Nonetheless, any non-UK trust acquiring land or property in the UK will be required to register on TRS. Furthermore, trusts already registered in another EU Member State will be automatically exempt from UK registration.

of beneficial ownership information, it is generally available only to specific competent authorities within the jurisdiction and public access to the information is limited. There is ongoing discussion about whether information in beneficial ownership registries should be made public.

Furthermore, a major criticism of public registers has been the lack of verification checks on recorded BO information. In September, Companies House announced reforms to introduce independent verification (but it has not yet set a timetable for these reforms).[3] These changes aim to provide businesses with greater assurance when they are entering transactions with other companies. If accepted, these proposed reforms would be one of the most significant transformations of the UK's company registration framework since the introduction of the register, some touching the core of the Companies Act. They will also improve the ability of law enforcement agencies by improving corporate transparency and the accuracy of information on the public register, thereby assisting in combatting economic crime and fraud.[4]

The Sixth Anti-Money Laundering Directive (6AMLD)

A further EU Anti-Money Laundering Directive ('6AMLD') will take effect on 3 December 2020. It introduces stricter punishments for money laundering, including maximum imprisonments. It provides more detail on possible offences, including concealing the source of illicit gains, and extends criminal liability to legal persons. The UK has opted out of the 6AMLD as the government considers it is already largely compliant with the Directive. However, while some of what is contained in 6AMLD is currently law in the UK, the introduction of a 'failure to prevent money laundering' offence is not currently within the scope of English law. Whether the UK is required to implement this new failure to prevent money-laundering rule will depend on the status of the transition period at the time. The Sixth Directive focuses on harmonising money laundering offences across the EU, such as extending criminal liability to legal persons and aiding and attempting to commit money laundering should be an offence. This is somewhat surprising, as it would mean the EU adopting a stricter approach to corporate criminal liability for money laundering than the UK, a jurisdiction that has taken a historically firmer approach. Whilst the member states are still grappling to ensure compliance with 6AMLD, the talks on the need of 7AMLD are already gaining heat.

Conclusion

The 2018 FATF report, 'Concealment of Beneficial Ownership', highlights the fact that increased global trade in a borderless commercial environment is now a major challenge for individual jurisdictions. The role (and effectiveness) of central registers of BOs in providing transparency is an ongoing debate, with public policy weighing in on what information should be made available to the public. Jurisdictions implement the international transparency standards in a

[3] The proposals for verification reform by Companies House are included in the government's response to the Corporate Transparency and Register Reform consultation that took place between May and August 2019. A government summary can be found here.

[4] See: https://www.gov.uk/government/news/reforms-to-companies-house-to-clamp-down-on-fraud-and-give-businesses-greater-confidence-in-transactions.

manner consistent with their national legislative and institutional systems. Further, the methods by which compliance with substance requirements can be achieved may differ from one jurisdiction to another. With global corporate tax rates generally falling, there is an increasing pressure on jurisdictions to strike a balance between ease of doing business and maintaining transparency and credibility of their regulatory framework.

The poster children of anonymity, shell companies are non-publicly traded corporations, limited liability companies and trusts that typically have no physical presence and have become common tools for money laundering, fraud and other criminal activities. A global joined-up regulatory approach is needed to target the vulnerabilities of a financial system that allows such structures to serve as a gateway to facilitate billion-dollar financial crimes of corruption, fraud and money laundering.

About the Authors

Anthony Riem is recognised as 'stellar practitioner' and leading lawyer in fraud investigation and litigation, asset recovery, banking litigation and commercial litigation. His tenacity in uncovering facts, which has won Anthony plaudits in the directories, is valued by clients when fraud requires investigation and the evidential picture needs to be built. He is a founding member and former Chairman of the Commercial Fraud Lawyers Association and an English member of Fraudnet. Anthony has an established practice acting for banks in multi-million dollar litigation, often involving freezing orders in several jurisdictions. In addition, he has been instructed in many leading commercial litigation cases over the years, at both first instance and appellate levels. Anthony's practice focuses on fraud investigation and litigation, asset recovery, banking litigation and commercial litigation.

Priyanka Kapoor specialises in multi-jurisdictional financial crime and regulatory matters. She has extensive experience of all issues related to bribery and corruption, money laundering, terrorist financing, economic sanctions and fraud. She has particular expertise in conducting complex internal investigations, and defending companies and individuals in regulatory investigations, both domestic and cross-border. She has worked on some of the most complex and high profile investigations in Asia. Priyanka regularly assists corporates, financial institutions and individuals with governance and compliance issues, helping identify and mitigate business risk. She also advises on due diligence in the context of cross-border corporate exercises and on the engagement of foreign agents and consultants. Priyanka has extensive experience of dealing with various sovereign regulators on behalf of clients. She has also advised regulators on the development and implementation of policies and regulations on business crime related issues. She has a deep understanding of the priorities and concerns of regulators and law enforcement authorities, which clients facing regulatory actions find enormously useful. Her experience spans a wide range of industry sectors, particularly, financial services, technology and natural resources. She has previously worked in Singapore, the US and India. She held leadership positions with two global banks and was a part the financial integrity group at the International Monetary Fund (IMF). She is admitted as a Solicitor in England & Wales.

Anthony Riem
Partner, PCB Litigation Solicitors

Email: ajr@pcblitigation.com
T: +44 (0) 7887 732 522

Priyanka Kapoor
Partner, PCB Litigation Solicitors

Email: pk@pcblitigation.com
T: +44 (0)7901 257 924

PCB LITIGATION SOLICITORS

The International Corporate Transparency Landscape: A Not So Silver Bullet?

Dr Dominic Thomas-James

Abstract

Corporate ownership secrecy has become firmly part of the global fight against economic misconduct, given the problems and investigative challenges presented by anonymous ownership, or by jurisdictions who do not keep or exchange beneficial ownership information. However, internationally, there remains ill-defined standards on how jurisdictions should achieve this – whether by a central, government-held register – or a (free) publicly-accessible one. As international momentum increases towards full transparency in this context, this paper reviews the international landscape and the extent to which there is parity and dissimilarity in approaches taken, often by perceivably similar jurisdictions. Public registers are now seen as a 'silver bullet' in fighting financial crime and tracing the concealment of assets facilitated by anonymous companies, while also providing a tool for enhanced risk management and due diligence. However, this paper highlights some of the shortcomings with the public register approach, the practical difficulties which will exist in terms of 'following the money', and unintended consequences which need to be addressed, that could stifle investigations and enforcement efforts.

Introduction

For some time, it has been widely acknowledged that anonymous legal entities can facilitate economic crimes such as serious and complex fraud, corruption, money laundering and terrorism financing.[1] Indeed, the task of lifting the corporate veil and understanding true ownership or control of companies is an increasingly crucial aspect of enforcement, recovery and, ultimately, the disruption and prevention of economically-acquisitive crime. This component of company law and regulation has traditionally been within the remit of domestic companies registrars. Today, the activity of keeping and exchanging beneficial ownership information is different depending on the jurisdiction in question, which is counterintuitive to the seemingly universally-accepted advantages of transparency. In recent times, the Panama and Paradise papers data-breaches emanating from

[1] Findley, M., Nielson, D. L., and Sharman, J. (2014) *Global Shell Games*, Cambridge: CUP.

law firms' offices in Panama and Bermuda have exacerbated momentum and support towards increased transparency. These events heavily influenced the passage of the public register provisions directed at UK Overseas Territories[2] in the Sanctions and Anti-Money Laundering Act 2018, with the utility of the data-breaches frequently cited.[3] The data-breaches and consequent publications created, essentially, a public register of sorts – notwithstanding fundamental legal concerns about how this information came to be published.

Standards Misaligned

Unhelpfully, there remains confusion about what an international standard on beneficial ownership information gathering, storing and exchanging is, or should be. From an outsider's perspective, given how forceful the U.K. and E.U.'s advocacy has been toward public registers, there is a *prima facie* case that public registers are fast becoming a 'global standard'. However, with pause, it is patently apparent that such an endeavour is in its infancy with the rate of buy-in from jurisdictions around the world.

Various sources of international hard and soft law suggest different standards. For example, the Financial Action Task Force ('FATF') – the international standard-bearer on anti-money laundering and counter-terrorism financing standards – suggests that countries should ensure there is accurate information held on beneficial ownership and that this be provided to competent investigative authorities.[4] Elsewhere, the 5th Anti-Money Laundering Directive of the European Union states that members must make this information available to any member of the general public.[5] This has to be taken against a backdrop whereby the 4th Anti-Money Laundering Directive indicated that members could hold the information either in a central (e.g. government held) or public register.[6] In such close succession, the E.U.'s own standard removed any reference to a central register standard.

The U.K. has had a public register for some time, with its publicly and freely accessible persons with significant control register operational since 2016. There, companies or their agents must provide information to Companies House as to the person(s) with significant control – in other words, the person who ultimately owns or controls the entity. This built upon an already public register of company officers and other information publicly-available. The U.K. government's advocacy on public registers has extended to its Overseas Territories and Crown Dependencies, which has been a source of tension amongst these groups of jurisdictions. Section 51 of the Sanctions and Anti-Money Laundering Act 2018 compels U.K. Overseas Territories to create public registers by the end of 2023, or face having them imposed by Orders in Council.[7] Many of the territories have developed into internationally significant financial centres such as Bermuda, Cayman Islands and the British Virgin Islands, and across the region opposition to this was unwavering on many bases including arguments relating to economic sustainability, respect for their Constitutions and

[2] For further background on the UK Overseas Territories in this context, see: Thomas-James, D. (2019) 'Beneficial Ownership and the UK Overseas Territories: More Haste, Less Speed?', *Company Lawyer* 40(8): 263-264.
[3] The debate on public registers in the UK Parliament demonstrates this, see: HC Deb (1 May 2018), Vol 640, Col 203.
[4] Recommendation 24, Financial Action Task Force AML/CFT Recommendations, available at:
[5] Directive 2018/843, Article 30(5)(c) as amended.
[6] Directive 2016/849, Article 30(3).
[7] Section 51, Sanctions and Anti-Money Laundering Act 2018 (UK).

democratically-elected legislatures, and disproportionality. However, perhaps surprisingly, 2020 saw a stream of high-level commitments and U-turns made whereby all the territories agreed to work towards implementing them in the timeframe. While section 51 of the 2018 Act only applied to the Overseas Territories and not the Crown Dependencies, given the latter have a different relationship with the U.K., the Crown Dependencies also made the same commitments to create public registers.

Traditionally, many of these jurisdictions have collected beneficial ownership information at government – or registrar – level, and have recently engaged in more onerous regulatory and reporting requirements on the part of corporate service providers and agents as required by FATF standards. Bermuda, for example, has collated beneficial ownership information for decades and has entered into numerous bilateral information exchange frameworks. Elsewhere, while making high-level commitments, the BVI avers that its Beneficial Ownership Safe Search System ('the BOSS System') is a viable alternative and safeguards fundamental legal rights such as confidentiality given that the system provides access to competent investigative authorities. Some jurisdictions, like BVI, have made these commitments based on various caveats such as exploring viable alternatives, and on public registers becoming a norm by the appointed time.

Despite advocacy at the U.K. and E.U. level, as recently as 2018, only 6 G20 countries were operating public registers[8] and at March 2020 only 5 EU Member states (including the U.K. for this purpose) operated them.[9] The U.S. is on the verge of creating a central register of beneficial ownership information under the recently approved provisions under the Corporate Transparency Act, however public accessibility to this is not yet on the agenda.

Effects of Increased Transparency

Proponents of increased transparency have commented on the usefulness of the Panama and Paradise papers in terms of enabling civil society to scrutinise entities registered in jurisdictions which do not operate public registers.[10] When considering effectiveness, however, there is significant difference between a spontaneous, without-notice dump of data – and giving users until 2023 to set their affairs in order, as it the case with the requirements under section 51 Sanctions and Anti-Money Laundering Act for the UK Overseas Territories.

Other forceful arguments relate to the 'Nothing to Hide'[11] conjecture – a utilitarian notion rooted in the concept that individuals who are not engaged in conduct which is illegal or untoward should have no issue with making their affairs visible on public registers. This argument does not account for the fact that even the strongest proponents of public registers acknowledge the protection provisions that exist should users be able to demonstrate, at a high hurdle, that their data being made public would cause significant harm or risk of harm.[12] The concept of scrutiny is a powerful argument for public registers, given the accepted nexus between the commission of financial crime

[8] Transparency International 'G20 Leaders or Laggards? Reviewing G20 Promises on Ending Anonymous Companies', available at: https://www.transparency.org/en/publications/g20-leaders-or-laggards#.
[9] Global Witness (2020) 'Patchy Progress in Setting Up Beneficial Ownership Registers in the EU', available at: https://www.globalwitness.org/en/campaigns/corruption-and-money-laundering/anonymous-company-owners/5amld-patchy-progress/ (data includes the UK).
[10] Supra 3, Col 203, Rt. Hon. Andrew Mitchell MP.
[11] Solove, D. J. (2008) "I've Got Nothing to Hide' and other Misunderstandings of Privacy', *San Diego Law Review*, 44: 745-772.
[12] Global Witness (2017) 'Learning the Lessons from the UK's Public Beneficial Ownership Register', [5].

and the ability to conceal ownership through anonymous companies. While those in our field may question both the legitimacy of the manner in which the Panama and Paradise papers information was obtained, and indeed may remain underwhelmed in terms of the fallout, they inarguably served a purpose in providing investigative lines of inquiry.[13] However, ethical and evidential difficulties exist with the data – forcing some enforcement bodies to reject invitations to view the files on the basis of ethical and professional concerns.[14]

The scrutiny function of public registers affords many parties (including investigators, investors and creditors) additional due diligence and risk management tools. While reliance on the public register in the U.K. is not enough in some professions to discharge customer due diligence requirements, the public register enables a cross-referencing ability and additional data-set resource. However, this presupposes that the information being scrutinised on the registers is accurate and truthful. For example, despite the U.K.'s register being world-leading, there remain considerable shortcomings relating to the lack of independent verification of information submitted on the register. This has caused Companies House to recently announce reforms to address such issues.[15] A lack of independent verification places a concerning reliance on the honesty, accuracy and timeliness of data provided by users or their nominated agents or representatives. If the concerns justifying public registers pertain to individuals or companies concealing assets from creditors, or using companies to launder illicit wealth, then not subjecting the data to independent verification misses the whole point of scrutiny. The information may simply be inaccurate or patently false. If an objective of transparency is to disrupt the behaviour of dishonest criminals, then giving them or their professional enablers the ability to provide false or misleading information to the registrar undermines any suggestion that public registers in and of themselves are a 'silver bullet' in disrupting criminal behaviour.

A final issue to note is the extent to which fundamental legal safeguards such as privacy and confidentiality are being eschewed in favour of increased corporate transparency. The whole development of the offshore industry has been built upon a notion of respect for privacy and confidentiality. Given the importance of this industry for the sustainable and economic development of many small-island nations including those in the Caribbean which are part of the UK Overseas Territories, increased regulation in this regard will doubtless have an impact on aspects of their narrow economies. This is particularly concerning for jurisdictions like BVI who operate a significant incorporation and corporate services market.

As Nakajima (2017) suggests, "a fundamental question we might ask ourselves is that even if we have nothing to hide, do we not wish to retain a certain level of confidentiality".[16] As Antoine (2014) notes, "the notion of a fiduciary relationship must be even stronger within offshore financial

---

[13] *New York Times* (28 July 2017) 'How the Panama papers changed Pakistani Politics', available at: https://www.nytimes.com/2017/07/28/world/asia/panama-papers-pakistan-nawaz-sharif.html.

[14] For example, the Swiss Government reportedly rejected the invitation to view the data in Germany, with its Attorney General's Office saying it was restricted by regulations on receiving and using evidence. See: *SwissInfo* (27 January 2019) 'Switzerland rejects German Panama Papers offer', available at: https://www.swissinfo.ch/eng/legal-restrictions_switzerland-rejects-german-panama-papers-offer/44712630.

[15] See: HM Government, Dept. for Business, Energy and Industrial Strategy (18 September 2020) 'Corporate Transparency and Register Reform'.

[16] Nakajima, C. (2017) 'The international pressures on banks to disclose information', in Booysen, S.A., and Neo, D. (eds) *Can Banks Still Keep a Secret? Bank Secrecy in Financial Centres around the World,* Cambridge: CUP.

circles where legitimate clients invest on the understanding of priority given to confidentiality".[17] Even the most ardent proponents of public registers often concede the legitimate use of offshore structures.[18]

Unintended Consequences

The whole point of increased transparency is to shine light on financial markets – particularly those known as offshore financial centres – which have been perceived and presented by international stakeholders as opaque and uncooperative with regards to economic crime, regulation and compliance. However, absent a coordinated effort and contemporary action by all jurisdictions which operate sophisticated financial centres, then the overnight push for public registers risks trying to solve a problem by creating another. One of the more concerning consequences of the fact that international standards are presently unaligned, is that it risks furthering the race to the bottom for illicit finance or concealed assets to jurisdictions which are harder to monitor, with operate structures in which tracing is more complex, where international cooperation may be minimal or non-existent, and where regulation is lacking. As those reading this paper will doubtless be aware, these jurisdictions *do* exist and contrary to the perception that UK Overseas Territories are the weakest links in the global financial system, there are a raft of jurisdictions with far less by way of legal infrastructure and international cooperation frameworks.

Summary

For any jurisdiction wanting to enhance its regulated environment, increasing transparency is a firm way of securing one's place in the international community. This is particularly so given the dearth of jurisdictions that have implemented public registers to date. They will have to, however, be set against a backdrop of increased regulatory oversight and reporting requirements, together with measures to adequately and independently verify data submitted to it. Otherwise, the effects may be in 'name only' and a nod to increased regulatory standards, rather than a substantive, useful tool which will assist in risk management, due diligence and the prevention and disruption of economic crime. The latter will only be realised if accompanied by independent verification and will not come close to resembling the 'silver bullet' that campaigners and Parliamentarians alike aver them to be. Otherwise, jurisdictions which have, in good faith, implemented central beneficial ownership registers combined with internationally-advocated bilateral information exchange frameworks, may rightly argue that their model is a viable alternative to the present landscape's pull towards public registers at any cost. After-all, there must be a distinction between information we have an "interest in" and that which is simply "interesting".

[17] Antoine, R-M. (2014) *Confidentiality in Offshore Financial Law,* Oxford: OUP, [26].
[18] See: ICIJ Disclaimer for the Panama & Paradise papers data, which states: *"There are legitimate uses for offshore companies and trusts. We do not intend to suggest or imply that any people, companies or other entities included in the ICIJ Offshore Leaks Database have broken the law or otherwise acted improperly…"*: https://offshoreleaks.icij.org/?gclid=Cj0KCQjA5bz-BRD-ARIsABjT4nhvrWkaQXS6aeVE1INliDrdozdAIzULfTofI4jWsXTF_7WSocXUiZsaAuNPEALw_wcB.

About the Author

Dr Dominic Thomas-James serves as the Editor of the inaugural FraudNet Global Report. He is presently the Course Director of the International Development programme at the University of Cambridge Institute of Continuing Education, a member of the Cambridge Centre for Criminal Justice (CCCJ), and is a Global Justice Fellow at Yale University. His research interests include economic crime, financial regulation, international and offshore financial centres. Dominic earned his Ph.D. and M.Phil. from Queens' College, Cambridge. He serves as a Secretariat Member of the Annual International Symposium on Economic Crime at Jesus College, Cambridge. He lectures widely and is frequently invited to speak at conferences and forums internationally. Dominic's written work is regularly published in peer-reviewed journals and he is the author of the forthcoming book *Offshore Financial Centres and the Law: Suspect Wealth in British Overseas Territories* (Routledge, 2021). He is regularly invited to serve as a consultant to various inter-governmental and international organisations. Dominic is also a barrister, called to the Bar of England and Wales by the Honourable Society of the Inner Temple, and is a Door Tenant at Goldsmith Chambers, London.

Dr Dominic Thomas-James
LL.B. (Hons), M.Phil., Ph.D. (Cantab), Barrister (Inner Temple)

Editor, FraudNet Global Report

E. dominicthomasjames@cantab.net

Part III

Complex and Commercial Fraud Including Bankruptcy and Insolvency Issues

Creditors Rights and Remedies in Guernsey, Channel Islands

John Greenfield, David Jones & Steven Balmer

Abstract

In this article, John Greenfield, Consultant, David Jones, Partner, and Steven Balmer, Associate, of the firm Carey Olsen examine innovative mechanisms by which creditors may seek to investigate secure assets held in Guernsey structures. In the second part of the article, the authors look particularly at companies and how the traditional insolvency regimes may be employed in aid of creditors but also at how the use of share security may unlock certain doors. However, in the offshore world it is often the case that the creditor is required to do some "trust busting" because the structure to be enforced against will involve a trust holding ownership/control of a holding company which in turn will control and own underlying companies/assets. The paper starts, therefore, with a real life example of how innovative advice helped protect creditors in such a structure.

1. Receivership Orders as an aid in asset recovery against trust assets

The problem to be resolved here is that the Guernsey trust is a legal entity in its own right and the shares of any company or other asset in the trust will be owned legally by the trustee. It is first essential to understand where the creditor fits in with what can be a complex structure and in particular with what parts of that structure has the creditor a legal relationship to enable it to enforce payment of the debt. More often than not, the debtor will be the settlor and/or the principal beneficiary of the trust and not the trustee. This creates a problem for the creditor who may not have a direct relationship – contractual or otherwise – with the trustee which actually is the owner of the assets to be recovered.

In this situation, Guernsey law has a common law remedy (very similar to the statutory regime in the United Kingdom) which will come to the rescue, providing the necessary circumstances exist. Essentially, it is necessary that the trust funds were placed in the trust when the settlor had good reason to believe that he would not be able to pay all his debts as they fell due. In this situation the Court will order the assets to become available for enforcement removing the legal ownership by the trustee even though the trustee was not the actual debtor.

Case Study

In the case where the trustee is actually the debtor in its capacity as trustee of a particular settlement different issues can arise. In the fairly unusual (and factually very complex) case of *Glenalla & Others v. Investec Trust Company Limited & Others* [2018] UKPC *7* , a settlement created for a Robert Tchenguiz and his family, different but urgent remedies were needed to protect the position of a creditor (the liquidators of the claimant companies – Grant Thornton) where the validity of the debt was in dispute. In other words, the creditor was not yet at the stage of being able to take any formal legal action to recover assets for payment of the debt but was still categorised as a "contingent creditor" until able to obtain a final undisputed Court judgment. In fact, it took over seven years and a hearing before the Privy Council in London before the creditors in this case became undisputed judgment creditors for a sum in excess of £200 million including interest.

The trust assets contained an eclectic range of investments and assets from Mr Tchenguiz's personal family home to highly geared derivative investments and credit default swaps. Many were highly sophisticated investments which needed very regular and frequent management and investment decisions during that seven year period. To further complicate matters, the settlor (Mr Tchenguiz) hired and fired the trustees on a number of occasions during the seven year period and the claimant creditors were not content to let investment decisions be taken by trustees seen to be firmly in the camp of the ultimate debtor. The claimant creditor needed to be able to exercise control over the investments whether that was to include sale, lease, further acquisitions, etc. The Guernsey Court, and ultimately the Privy Council, were faced with an extremely interesting challenge in finding the right balance between the interests of the beneficiaries of the trust (should the claimant's action ultimately fail) and the interest of the creditors.

The Guernsey Court determined that the answer lay in applying a type of Receivership regime which bore certain similarities to that found in relation to companies. From late 2012 until the Privy Council hearing in 2018, Carey Olsen succeeded in obtaining and holding Court Orders whereby all but the Tchenguiz family home was transferred into the legal ownership and control of a professional receiver/insolvency practitioner nominated by the creditors (and therefore removed from the control of the trustees). This was an extremely important and innovative approach by the Guernsey Courts and gave the creditors considerable comfort that the assets upon which they were wishing to enforce once judgment had been confirmed would still have the value that they could reasonably expect.

This is a classic example of the Courts applying a flexible solution to aid the creditors up to the time of enforcement when other normal remedies would then come into play. We now turn to look at Guernsey's statutory insolvency regime as part of the recovery toolkit and the proposed changes to it.

2. The Guernsey Insolvency Regime as an aid to asset recovery - companies

The key to a successful fraud investigation and subsequent recoveries is often the speed with which control can be asserted over companies, their management, assets and records. The Guernsey insolvency regime, if utilised correctly, offers effective tools in that control-taking process.

Overview of available procedures

Guernsey's corporate insolvency regime is contained within the Companies (Guernsey) Law 2008, as amended (the **Companies Law**). The Companies Law provides for three insolvency processes, namely: administration, voluntary liquidation and compulsory liquidation. The regimes will be broadly similar to those familiar with the English insolvency regime save for a number of fundamental differences that may offer assistance in fraud investigations or with asset recoveries.

Administration

A company may be put into administration at the request of the company, the directors of the company, any member of the company, any creditor of the company (including contingent or prospective creditors), and the Guernsey Financial Services Commission. Guernsey statutory administration provisions are contained at Part XXI, ss.374 to 390 of the 2008 Law. The Royal Court has jurisdiction to make an administration order if satisfied that:

- the company concerned "*does not satisfy or is likely to become unable to satisfy the solvency test*" [see s.374(1)(a)]; and
- the "…*making of an order under this section may achieve one or more of the purposes set out in subsection (3)*" [see s.374(1)(b)].

The "*purposes*" which an administration order seeks to achieve under s.374(3)(a) and (b) are:

- the "*survival of the company and the whole or any part of its undertaking, as a going concern*", **or**
- a "*more advantageous realisation of the company's assets than would be effected on a winding up*".

The main effect of an application for an administration order would be the implementation of a court sanctioned moratorium against resolutions for the winding up of the company, and on the commencement or continuance of proceedings against the company concerned (without leave of the court) during the period between the presentation of the application and the making of the actual administration order. The granting of the administration order itself would provide the company with the continued benefit of this moratorium (save with the consent of the administrator or leave of the court). Critically, however the moratorium does *not* affect a secured creditor's right to enforce its security.

Compulsory Winding Up/Liquidation

The main grounds for the compulsorily winding up of a company are that *inter alia:*

- the company is unable to pay its debts within the meaning given in s.407 of the Companies Law or otherwise fails the 'solvency test'; or
- the court is of the opinion that it is "*just and equitable*" that the company be wound up.

An application for the compulsory winding-up of a company may be made to the Court by the company, any director, member, creditor or any other "*interested party*". There is no need for a detailed analysis of the liquidation regime for the purposes of this article given its effect will be

familiar to most, *i.e.* it triggers a starting gun for a realisation of assets and payments in accordance with the statutory order of priorities. It does, however, hand control of the company to a third party liquidator who will be afforded investigatory powers (as to which see later) and certain statutory remedies with regard to antecedent transactions and delinquent conduct of directors.

Voluntary Winding Up

A Guernsey company may be voluntarily wound up by means of a special resolution of its shareholders (passed by a majority of 75%). A copy of the special resolution must be filed at the Guernsey Companies Registry within 30 days who will publish notice on its website. The process can be utilised in respect of insolvent companies albeit it is purely shareholder-driven and does not involve any Court supervision. The process is very light-touch in terms of creditor and member engagement, and is designed to serve as a simple mechanism for finalising a company's affairs.

The company must appoint a liquidator by ordinary resolution (passed by a majority of 50% plus 1) to wind up the affairs of the company and fix his remuneration. This can be done in the same special resolution resolving to wind up. The liquidator need not be a qualified insolvency practitioner nor resident in Guernsey. In fact it can be any legal person and there is currently no need for independence. Whilst there is obvious risk of abuse of the regime in those circumstances, it also offer a route into a Guernsey company for an overseas insolvency practitioner who may be appointed in another jurisdiction to an overseas parent or may be engaged by a concerned creditor holding security over the Guernsey company's shares.

Incoming Changes to the Guernsey Insolvency Regime

In January 2020, the States of Guernsey approved the Companies (Guernsey) Law, 2008 (Insolvency) (Amendment) Ordinance, 2020 ('the Ordinance'). The Ordinance was designed to further enhance Guernsey's reputation as a robust jurisdiction for restructuring and insolvency. Among the many key changes being introduced is the introduction of new powers for liquidators who will be able to compel the production of documents from directors and officers and to appoint an Inspector of the Court to examine directors and company officers. The proposed changes presented a significant "beefing up" of the statutory investigatory powers available to insolvency office holders in Guernsey bringing them broadly in line with those available under the section 235 and 236 of the English Insolvency Act 1986. This ability to compel the production of information and documentation will prove a vital tool in any investigation of wrongdoing and subsequent recovery action.

A further important change will be the introduction of a formal statutory remedy by which office holders will now be able to pursue recovery of transactions at an undervalue and extortionate credit transactions - a power notable by its absence in the current regime.

Another important change is the ability to wind up a non-Guernsey company. Under the existing regime, there is no ability for the Royal Court to wind up a non-Guernsey registered company. In light of Guernsey's modern status as an international finance centre providing administration and asset management services to many foreign companies, this was a lacuna in the law which has now been filled. This change brings Guernsey in line with other major jurisdictions

and will allow the Royal Court to apply the Guernsey regime to foreign companies where they have a sufficient connection to the jurisdiction. It provides comfort to those doing business with entities operating or with assets in Guernsey but not registered here, that they will have access to the jurisdiction's insolvency regime if necessary.

Finally, we examine an often overlooked tool in terms of securing control in the form of enforcing share security.

Using Share Security to Take Control

Security over shares in a Guernsey company must be created by a security interest agreement that complies with the Securities Interests (Guernsey) Law, 1993 (the 'Securities Law'). Typically, the security will involve possession of the share certificates and an assignment of the voting rights. In the event of a default in the lending sufficient to crystallise enforcement remedies, the Securities Law only specifies a power of sale or application as the only available method of enforcement. There is no concept of receivership in Guernsey in this context. As such, the security holder will have the right to take possession of the shares in discharge of a debt or with a view to a sale of them Guernsey's statute is express in not requiring Court approval for the exercise of the statutory powers of sale or application.

In a normal enforcement scenario in default of a debt, the security holder may look to sell shares to pay down debt or may consider applying the shares by housing them in some other vehicle to enable it to realise value whilst preserving the group structure. However, where there are concerns about the activities of management and potential fraud, share security may also offer a quick and effective route to denude delinquent directors of control but also to secure information for investigative purposes. Ultimately, the liquidator may also be afforded statutory causes of action to recover assets otherwise unavailable to a shareholder.

One way in would, of course, be for a security holder to take possession of shares and "perfect" its security by demanding that it be placed onto the shareholder register pursuant to its possessory rights. In that way, the security holder would become the shareholder of record and would be able to exercise all voting rights attaching to the shares accordingly. However, taking this step may present its own challenges in terms of ensuring compliance by the company or its corporate administrator and in terms of the security holder having the appetite for taking ownership of shares. For example, it is unlikely that a retail bank will acquiesce to becoming the owner of shares in an offshore structure.

Whilst there are ways around the ownership conundrum, about which we could write a separate paper, there is another potential option. The security documents themselves will provide a host of powers for the lender to assist it in the enforcement of the security. Those powers will often include the right to direct the borrower to vote the shares in a particular way and an acknowledgment from the company itself that it will comply with that direction. The documents may also give a power of attorney to the security holder to exercise its rights without recourse to the company.

As a result, the holder of the security may be able to exercise the voting rights which in turn may permit it (dependent on the percentage shareholding it controls) to:

- replace a board or appoint a director; or
- commence a voluntary liquidation process and appoint a liquidator to take control of the company.

As set out above, this is particularly useful in Guernsey where the voluntary winding up process can be used without a declaration of solvency, i.e. for an insolvent company in terms of giving control and access to records. The remedy is also instant in that the appointment will commence the moment the resolution is passed and as such circumvents the time involved in the Court process. The option always remains to convert a voluntary liquidation to a compulsory at a later date by application to the Court.

This method has been successfully used for Guernsey entities that own UK real estate where there is a default in the lending that has led to the appointment of a LPA receiver a UK real estate asset but gaining control of the holding company is important for information gathering or to prevent the incumbent directors from undermining the receivership.

There are, of course, issues to be considered in advance of using the security powers not least, the statutory requirements that may go along with a change of shareholder. For example, The Beneficial Ownership of Legal Persons (Guernsey) Law 2017 requires the resident agent of a company to take reasonable steps to ascertain the identity of the beneficial owners of a company and keep records of them. Security holders have to be prepared to provide CDD information this CDD information if they are to be entered onto the share register. However, utilising share security is an often overlooked tool in the box that can be very effective.

Summary

Guernsey has pursued a policy over many years now to be user friendly to creditors seeking to recover the debt owed to them by entities subject to Guernsey Court jurisdiction, whether companies or trusts. The creditor has an array of weapons in his armoury and should not be afraid to use them.

About the Authors

John Greenfield is a consultant at Carey Olsen in Guernsey, where he was previously senior partner. John undertakes the complete range of major litigation and advocacy work including asset tracing, multi-jurisdictional disputes and commercial and trust litigation. John has been counsel in many of the major litigation cases before the Royal Court of Guernsey and the Guernsey Court of Appeal and is one of the few Guernsey advocates to have appeared as counsel in the Privy Council. John was a founder member of the Guernsey Royal Court Working Party which completely reviewed the island's Civil Procedure in 2008 and is a member of the UK Fraud Advisory Panel. He is a founder (and only Guernsey member) of Fraudnet and is a member of the Association of Contentious Trust and Probate Specialists (ACTAPs) and is a Notary Public. He features in the Legal 500 UK, 'Hall of Fame' for Dispute Resolution.

David Jones is a partner at Carey Olsen and a Guernsey advocate, providing specialised advice in relation to business restructuring and insolvency in contentious, non-contentious and multi-jurisdictional matters. He has been involved in many of the largest insolvencies involving Guernsey entities, ranging from investment funds to global retailers. He is able to assist lenders in respect of the taking and enforcement of all forms of security. David regularly advises the boards of distressed entities and has extensive experience acting for office holders. He is a member of the Insolvency Lawyers Association and R3 and sits on the young members Committee of INSOL International. David lectures on INSOL's Foundation Certificate in International Insolvency and is part of the working group tasked with updating and revising Guernsey's insolvency laws. He

has also been appointed as a member of Guernsey's first ever Insolvency Rules Committee (IRC). He is ranked in the Legal 500 UK, 2020 edition for Dispute Resolution as a 'Next Generation Partner'.

Steven Balmer is an associate at Carey Olsen in Guernsey, who specialises in commercial litigation and insolvency matters as well as employment law. He works on a range of high-value commercial cases, contentious multi-jurisdictional litigations and insolvencies for both domestic and international clients including the Tchenguiz Discretionary Trust litigation and the liquidation of Joannou and Paraskevaides (Overseas) Limited. Steven trained with a national firm in Scotland and prior to that, spent two years working at the Judicial Institute of Scotland. He is a member of INSOL, the Guernsey International Legal Association (GILA), the Association of Restructuring and Insolvency Experts (AIRES) and the Asset Recovery Next Gen Association.

John Greenfield
Consultant

Carey Olsen
T. +44 (0) 1481 732026
E. john.greenfield@careyolsen.com

David Jones
Partner

Carey Olsen
T +44 (0) 1481 741554
E. david.jones@careyolsen.com

Steven Balmer
Associate

Carey Olsen
Tel +44 1481 741548
E. steven.balmer@careyolsen.com

CAREY OLSEN

British Virgin Islands – A Pro-Creditor Jurisdiction? A Review of Recent Case Law and Legislative Developments

Shaun Reardon-John

Abstract

Despite the British Virgin Islands (BVI) from time to time being on the receiving end of external criticism about its provision of offshore services and its reputation for maintaining confidentiality, it is in fact a flexible, creditor-friendly jurisdiction that has recently been in the headlines as a result of the Eastern Court of Appeal's decision which reversed the Court's well-established jurisdiction to grant injunctive relief in aid of foreign proceedings (known as *Black Swan* injunctions). In response, the BVI legislature moved swiftly to plug the gap left by Court of Appeal's decision by passing the Eastern Caribbean Supreme Court (Virgin Islands) (Amendment) Act which came into force on 6 January 2021. This is a further example of progressive steps being taken by the BVI legislature which creditors should be aware of. In this article, Martin Kenney and Shaun Reardon-John, of Martin Kenney & Co. Solicitors review the current and future direction of the BVI offshore legal system from a creditor perspective.

Black Swan jurisdiction

In the BVI, a 'Mareva injunction' (more commonly known as a freezing order) is granted pursuant to section 24 of the Eastern Caribbean Supreme Court (Virgin Islands) Act 1969 ('the 1969 Act'), which gives the BVI court the jurisdiction to grant injunctions in cases where, among other things, it appears to be just and convenient to do so. The main aim of a freezing order is to ensure that assets are preserved pending the outcome of the litigation so that they may be used to satisfy a future judgment.

Part 17 of the Civil Procedure Rules 2000 fleshes out the common law and statutory authority. Part 17.1(1)(j) allows the Court to make an order restraining a party from dealing with their assets regardless of whether they are located within the jurisdiction or not. Part 17.4 allows the Court to grant worldwide freezing orders (where assets located outside of BVI could be frozen as well, subject to the assistance of foreign courts), whether or not the respondent is domiciled or present within the BVI.

The decision in ***Eastern Caribbean Industrial Corporation Berhad v Vela Financial Holdings Limited*** [1], sets out the Court's wide discretion when considering whether to grant a freezing order to ensure that balance is given to the parties' rights. The reason for this is that freezing orders have been observed to be oppressive and expensive for respondents and third parties. As such, if granted, safeguards are usually put in place by the Court. Courts will also often order ancillary disclosure relief to ensure that the freezing order is effective. In ***Emmerson International Corporation v Renova Holding Ltd***[2], the Privy Council confirmed that asset disclosure provisions are an inherent part of effective freezing order relief.

The standard practice in the BVI prior to 2010, was that a freezing order could only be granted ancillary to a substantive domestic cause of action. There were some exceptions to this general rule, but they were not always easy to navigate, and so very often applicants failed in their efforts to freeze assets in the BVI in aid of foreign proceedings. The case of ***Black Swan Investments ISA v Harvest View Limited***[3] revolutionised the jurisdiction of the Court to grant orders in aid of foreign proceedings. In *Black Swan* the Commercial Court held that where the respondent was within the *in personam* jurisdiction of the BVI Courts, it had a discretion to grant freezing injunctions in support of foreign proceedings. In ***Yukos CIS Investments Limited v Yukos Hydrocarbons Investments Limited***[4] the Court of Appeal affirmed this decision.

The implications of the Convoy decision for the BVI if it had been allowed to prevail

Black Swan was seen as a major coup by pro-creditor practitioners in the commercial sector. It changed the landscape for a jurisdiction with over 400,000 active registered companies, the majority of which conduct business in foreign jurisdictions. The decision sent a message to the commercial world that debtors could not hide assets in the BVI and think they were unreachable by creditors. Not only did the Black Swan jurisdiction allow standalone freezing injunction claims, but Bannister J confirmed the Black Swan jurisdiction extended to prevent non cause of action defendants from dissipating identified assets which might be available to satisfy a future foreign judgement made against the primary (cause of action) defendant.

In the recent case of ***Convoy Collateral Limited v Broad Idea International Limited & Cho Kwai Chee***[5], the Court of Appeal held that there is no statutory authority under s.24 of the 1969 Act to grant an injunction in aid of foreign proceedings.

In this case, Justice Blenman summarised the principal issues for determination by the Court, namely:

[1] BVIHVC 2005/0046
[2] [2019] UKPC 24
[3] BVIHCV (COM) 2009/0399
[4] HCVAP 2010/028
[5] BVIHCMAP2019/0026

1. Whether in the absence of statutory provisions, it is possible for the Court to grant a freezing injunction against a person against whom there is no cause of action in any part of the world;

2. If so, whether the jurisdiction extends to granting a freezing injunction in support of foreign proceedings to which the person is not a party; and

3. Even if this is so, whether the learned Judge at first instance properly exercised his discretion in granting the freezing injunction.

Chief Justice Pereira compared the BVI to jurisdictions in which the legislature has taken steps to expressly give the Court's the jurisdiction to grant injunctions in aid of foreign proceedings. In England and Wales, s.25 of the UK Civil Jurisdiction and Judgements Act 1982 was passed. In the Cayman Islands, the courts are empowered under s.11A of the Cayman Islands Grand Court Law. Additionally, in the BVI, s.43 of Arbitration Act 2013, which post-dates the Black Swan decision, states:

> *"On the application of a party, the Court may, in relation to any arbitral proceedings which have been or are to be commenced in or outside the Virgin Islands, grant an interim measure."*

Having considered the above examples, the Court of Appeal concluded that:

> *"[50] …that the courts of the BVI, though having in personam jurisdiction over Broad Idea, being a BVI registered company, have no subject matter jurisdiction to grant a free standing interlocutory injunction against it in aid of foreign proceedings, there being no statutory basis for the exercise of such a jurisdiction. It is for the Legislature of the BVI to step in and clothe the court with such authority."*

The Court of Appeal's apparent dissatisfaction with the practical result of its determination appears to have been echoed by the Privy Council itself which, on 30 September 2020, stayed the Court of Appeal's decision and reinstated the Black Swan injunction pending its final determination of the matter. This was a highly unusual course of action which, we consider, highlighted the seriousness with which the alleged lack of statutory authority was being taken by the Privy Council.

Since the handing down of the Court of Appeal's decision, its reasoning, and the implications of it, have been a hot topic among legal practitioners. This article would be many pages longer if we were to consider all the potential ramifications and arguable defects of the judgment. However, even at a basic level, many consider the Court of Appeal made a fundamental mistake in interpreting s.24 of the 1969 Act which states:

> *"A mandamus or an* ***injunction may be granted*** *… by an interlocutory order of the High Court or of a judge thereof* ***in all cases in which it appears to the Court or Judge to be just or convenient*** *that the order should be made and any such order may be made either unconditionally or upon such terms and conditions as the court or judge thinks just." (emphasis added)*

Based solely on the ordinary meaning of the words, there is no requirement for there to be an underlying domestic cause of action against the respondent to the injunction application. The background of injunctive relief can be traced to the Chancery Courts of England and Wales. Section

24 merely confirmed the historic powers held by the Court. Why the Court of Appeal felt the need to diminish this power (ignoring 10 years of authorities relying on Black Swan Judgment), has baffled many practitioners.

To mitigate the potentially significant implications of the Court of Appeal's decision, the BVI government worked alongside the local legal community to produce a short but highly important piece of legislation. Most practitioners concerned by the Court of Appeal's judgment were able to breath a collective sigh of relief when the BVI Government passed the Eastern Caribbean Supreme Court (Virgin Islands) (Amendment) Act which came into force on 6 January 2021. The Act amended section 2 and inserted a new s.24A into the 1969 Act. The only question that remains for the Privy Council's consideration is whether the common law jurisdiction should remain intact alongside the new legislative jurisdiction.

The BVI's progressive legislative initiatives

There is no doubt that while the Convoy judgment created uncertainty for creditors seeking to protect their interests often against foreign judgment debtors, the swift implementation of the new legislation should be applauded. By design, money laundering is often cross-border in nature and the Black Swan jurisdiction went some way towards redressing the practical balance that had historically favoured the wrongdoer.

Further steps to ensure fraudsters are not able to utilize BVI companies for dishonest purposes are taking place via a draft Proceeds of Crime (Civil Recovery and Investigations) Act. This statute will ensure that steps can be taken to preserve and recover proceeds of criminal conduct without the authorities first having to secure a criminal conviction. 2020 also saw the introduction of the Charging Orders Act, a progressive piece of legislation that takes an expansive view of a debtor's interest in property.

Open registers – more harm than good?

These recent legislative initiatives and a noticeable fall in companies being incorporated in the BVI are interesting when considering the call for an open company register from outside the BVI. It is no secret that anonymous companies are often used to mask corrupt practices. The BVI has always been the focus of those who argue that closed registers of beneficial ownership information encourage financial crime, asset concealment and tax evasion.

In response to increasing pressure from the European Union ('EU'), in 2017 the BVI legislature enacted the Beneficial Ownership Secure Search System Act 2017 ('Boss Act'), a non-public beneficial ownership register. Following on from this initiative, the BVI enacted the Economic Substance (Companies and Limited Partnerships) Act 2018 which came into effect on 1st January 2019.

International law agencies now have access to information on the BOSS system at very short notice. This is a little-known fact rarely reported by the press when commenting on the BVI's offshore

financial industry. Instead, the BVI and other offshore jurisdictions are being targeted by the EU, which argues that open public registers are a necessity. A failure to comply is met with the threat of financial blacklisting, with all the negative connotations that has. It is this pressure that may have contributed to the BVI confirming it will adopt open registers by 2023.

Some people have questioned the EU's push for open registers given its own "offshore industry" onshore in Luxembourg.[6] The United States is in a similar position when one considers how difficult and expensive it is to obtain beneficial ownership information for companies incorporated in Delaware.

London has also been in the media recently as a result of the FinCEN leak[7] which exposed that company formation details are rarely verified[8] and fraud is rife. However, the FinCEN leak exposed not only the US and UK, but the entire financial sector, also painting the banks in a bad light. As an outsider it appears that the banks are either (a) swamped with dubious customers but are happy to carry on transacting with them, relying on the suspicious activity report "get out of jail free card" or, b) are concerned so much about missing a fraud that every minor concern is filed as a suspicious activity report to cover their backs. Regardless, the result is that FinCEN receives around 3 million suspicious activity reports every year. In addition to this, given the criticism that such reports are badly drafted and take time to decipher, it is unlikely that FinCEN could review all the information it receives. If it did, any fraudulent proceeds may have been laundered and/or dissipated by the time action is taken. Meanwhile, the banks continue transacting and profiting.

It is arguable that the BVI currently captures more accurate data than all of the three jurisdictions mentioned above. A recent article suggested that there has been a fall in BVI incorporations in recent years. However, perhaps more significant is the fact that the average lifespan of a BVI company appears to be increasing. This could be a sign that the increased UBO due diligence carried out by the BVI is deterring those who would seek to use incorporations for unlawful purposes from incorporating in the territory in the first place[9]. When faced with this information, some in the offshore world consider that these larger countries and organisations are seeking to squeeze out the smaller offshore jurisdictions, destroying the economies they have created, while failing to impose the same level of due diligence and transparency in their own jurisdictions. It is also felt that the British Overseas Territories are falling victim to the economic war that appears to be developing between the UK and the EU as a result of the EU allegedly wanting to punish the UK for leaving the EU, and by doing so deterring other EU nations from leaving[10].

---

[6] http://taxjustice.lu/archives/2011
https://fsi.taxjustice.net/PDF/Luxembourg.pdf
[7] https://www.bbc.co.uk/news/uk-54226107
[8] https://www.theguardian.com/world/2019/jul/05/how-britain-can-help-you-get-away-with-stealing-millions-a-five-step-guide
[9] https://www.bvibeacon.com/incorporations-still-falling-after-20-year-lows-in-2019/
[10] https://www.theparliamentmagazine.eu/news/article/hansolaf-henkel-eu-trying-to-punish-uk-in-brexit-talks
https://www.politicshome.com/news/article/philip-hammond-warns-eu-against-punishing-the-uk-in-brexit-negotiations
https://www.independent.co.uk/news/uk/politics/brexit-talks-senior-german-mep-eu-negotiators-punish-britain-hans-olaf-henkel-theresa-may-michel-barnier-a7848221.html

Supporters of open registers argue that it strengthens global transparency for the private sector and will lead to increased tax revenue. It is true that while the BOSS system has its benefits, national agencies will not have the time to monitor all complaints made against offshore entities. Indeed, a verified, accurate open register may make our day-to-day work easier. However, our experience has been that those seeking to evade the spotlight will merely put forward trusted nominees as the beneficial owners whereas previously they may have provided accurate information. Again, the unintended consequences of open registers could be that the information available to enforcement agencies becomes less accurate in some critical cases. An alternative option to open registers could be for government agencies to work with approved private sector companies who are given access to the BOSS system.

Concluding Thoughts

The BVI legislature's swift action to address the lacunae in the law caused by the Court of Appeal's judgment in *Convoy* sends a clear signal that the BVI is striving to keep pace with those who seek to evade justice by arming creditors with the necessary tools to preserve assets that may be subject to enforcement proceedings. As recent data leaks have shown, fraud is active and flourishing in financial centres across the globe. Perhaps authorities should be focusing not on opening public registers when there are systems like the BOSS in place but, rather, they should be asking why banks in the US are making circa 3 million suspicious activity reports a year, which are difficult to decipher and are overwhelming those authorities tasked with reviewing the data. Perhaps it is also time for all suspicious activity reports to be made public so that those members of the public who wish to investigate alleged suspicious activity can do so, rather than permitting them to trawl through legitimate offshore company data. It may also lead to less suspicious activity reports being filed if the banks are open to criticism from their clients for failing to properly consider facts before filing potentially damaging reports.

About the Author

Shaun Reardon-John is a Consultant Solicitor Advocate at Martin Kenney & Co Solicitors. He has particular expertise in cross-border insolvencies, fraud, asset recovery and commercial dispute resolution. He has acted on behalf of liquidators in relation to two cross-border insolvencies that involved international investigations where investors lost in excess $50 million. Shaun also worked as part of a team in relation to an international Ponzi scheme involving a failed financial institution.

In addition, Shaun has commercial arbitration experience involving two corporate parties regarding a breach of contract. Shaun has also been instructed in relation to the enforcement of arbitration awards with a cross-border nature.

Shaun Reardon-John
Consultant Solicitor Advocate
Martin Kenney & Co Solicitors
British Virgin Islands
T. +12843942444
E. sreardonjohn@mksolicitors.com

Martin Kenney & Co.
Solicitors

Redefining Reflective Loss – the Long Awaited Decision of the Supreme Court in *Marex*

Anthony Riem & Catherine Eason

Abstract

In this article, Anthony Riem, Partner, and Catherine Eason, Senior Associate, of the London firm of PCB Litigation review the fallout from the long-awaited and landmark Supreme Court decision in *Sevilleja v Marex*. In doing so, the authors outline the background and historical development of the principle of reflective loss by reference to its application in decided cases. The paper goes on to analyse the fallout from *Marex* set against former authority, but also the practical impact for practitioners and creditors of the Supreme Court's decision.

Redefining Reflective Loss – the long awaited decision of the Supreme Court in *Marex*

The rule against reflective loss has long been the subject of contention and criticism. When the Court of Appeal in *Sevilleja v Marex*[1] unusually gave permission to appeal from its own decision, the stage was set for a significant change to the law regarding reflective loss.

In what can only be described as a landmark decision, seven Supreme Court judges agreed that the continual expansion of the so-called "principle" of reflective loss has had unwelcome and unjustifiable effects on the law,[2] and were unanimous that the rule against reflective loss should not apply to claims by creditors. As a result, the appeal was allowed.[3] The wider question of whether reflective loss should apply to claims by shareholders proved divisive, and comprised a significant portion of the three judgments. The majority decided not to abolish the rule but established a "bright-line", restricting the scope of its application to losses that are merely reflective of losses suffered by a company. A minority took a step further and questioned whether the rule against reflective loss should ever apply.

[1] [2018] EWCA Civ 1468; [2019] QB 173
[2] As noted by Lord Hodge at [95].
[3] *Sevilleja v Marex* [2020] UKSC 31.

The Principle of Reflective Loss

The reflective loss principle was first identified and relied upon nearly 40 years ago in *Prudential Assurance Co Ltd v Newman Industries Ltd (No.2).*[4] The application of reflective loss has been both controversial and, at times, inconsistent. The decision of *Johnson v Gore Wood & Co*[5] took the reasoning from *Prudential* and advanced a number of other justifications for the exclusion of shareholder's claims in circumstances where a company has a concurrent claim against it. These principles were subsequently applied to claims brought by a claimant in the capacity of a creditor of a company, where he or she also held shares in it, and the company had a concurrent claim.

An exception ultimately arose in the case of *Giles v Rhind,*[6] where the Court of Appeal allowed the claimant (who was a former director and shareholder in the company) to bring proceedings in circumstances where the wrongdoing of the third party made it impossible for the company itself to recover the loss in question.

Shortly after the decision of *Giles,* the Court of Appeal in *Gardner v Parker*[7] reverted to a wide application of the principle, finding that reflective loss applied to a claim arising from a creditor's inability to recover a debt owed to it by a company in which the creditor was a shareholder. Lord Neuberger added that the same reasoning should apply even where the employee or creditor was not also a shareholder.

Since *Gardner v Parker,* the Courts have followed the approach adopted in that case. The reflective loss principle has been treated as based primarily on the avoidance of double recovery and the protection of a company's unsecured creditors, and as being applicable in all situations where there are concurrent claims and one of the claimants is a company. Its application was extended wider, with a number of judges commenting on both the uncertainties and difficulties of this doctrine. The decision of the Court of Appeal in the present case was the first case in this jurisdiction in which reflective loss has been applied to a claimant which is purely a creditor of a company.

The facts in *Marex*

A dispute arose between Mr Sevilleja and his two BVI companies ("Companies"), and Marex Financial Ltd ("Marex"), a foreign exchange broker. Marex brought proceedings against the Companies for amounts due to it under contracts which it had entered into with them. Following a trial in the Commercial Court, Field J had provided a confidential draft judgment to the parties, finding that the Companies were liable to Marex for US$5 million and costs of £1.65 million. Marex alleged that, following the release of Field J's draft judgment, Mr Sevilleja wrongfully asset-stripped the Companies by procuring the transfer of US$9.5m from the Companies' accounts in London to accounts in his personal control. The object of the transfers was to defeat payment of the Field J judgment, and as a result of the transfers, the Companies were placed into voluntary liquidation. The Companies were unable to pay the judgment debt that they owed Marex, and Marex claimed the judgment debt as damages against Mr Sevilleja in addition to interest and costs.

---

[4] *Prudential Assurance Co Ltd v Newman Industries Ltd (No 2)* [1981] Ch 204.
[5] [2002] 2 AC 1.
[6] [2003] Ch 618.
[7] [2004] EWCA Civ 781; [2004] 2 BCLC 554.

The appeal derives from an application for service of proceedings on Mr Sevilleja outside of the jurisdiction, which was appealed by Mr Sevilleja on the basis that Marex did not have a good arguable case against him. One of the arguments in support of this was that the losses which Marex was seeking to recover were reflective of loss suffered by the Companies which had concurrent claims against him, and were therefore not open to Marex to claim. Mr Justice Knowles held that Marex had a good arguable case that its claim was not precluded by reflective loss, and accordingly dismissed Mr Sevilleja's application.[8] On appeal, however, the Court of Appeal accepted that the "reflective loss" principle applied to about 90% of Marex's claim.

The Supreme Court Decision

In the majority decision, Lord Reed made it clear that crucially the position of a shareholder and a creditor is different. Specifically, a shareholder has a variety of other rights which may be relevant in a context of this kind, including the right to bring a derivative claim to enforce the company's rights if the relevant conditions are met, and the right to seek relief in respect of unfairly prejudicial conduct of the company's affairs.[9] There is, however, no analogous relationship between a creditor and the company.[10]

A distinction was also drawn where a company goes into insolvency. The shareholder will only recover a *pro rata* share of the company's surplus interest, with their share value reflecting the value of that interest. However the extent to which the company's loss may affect a creditor's recovery of his debt will depend not only on the company's assets but also on the value of any security possessed by the creditor, on the rules governing the priority of debts, and on the manner in which the liquidation is conducted. Most importantly, even where the company's loss results in the creditor also suffering a loss, he does not suffer the loss in the capacity of a shareholder, and his pursuit of a claim in respect of that loss cannot therefore give rise to any conflict with the rule in *Foss v Harbottle* (which states that the only person who can seek relief for an injury done to a company, where the company has a cause of action, is the company itself).

Lord Reed therefore reaffirmed the approach adopted in *Prudential* and by Lord Bingham in *Johnson*, from which it follows that *Giles v Rhind*, *Perry v Day* and *Gardner v Parker* were wrongly decided. The rule in *Prudential* is limited to claims by shareholders where as a result of actionable loss suffered by their company, the value of their shares, or of the distributions they receive as shareholders, has been diminished. Other claims, whether by shareholders or anyone else, should be dealt with in the ordinary way. This appears to create an opportunity for shareholders to bring claims where they can show that their losses were not in their capacity as shareholder, which are a consequence of losses to the company.

Lord Sales (with whom Lady Hale and Lord Kitchen aligned) agreed that there is a clear distinction between the application of the reflective loss principles to shareholders and creditors: a creditor of a company has not chosen to be in a position where he is required to follow the fortunes of the company in the same way as a shareholder.[11] However, he would not follow *Johnson* in so far as it endorsed the reflective loss principle identified in *Prudential* in relation to claims by shareholder

[8] [2017] EWHC 918 (Comm); [2017] 4 WLR 105.
[9] [83].
[10] [85].
[11] [198].

claimants, which he described as a "crude bright line" to exclude shareholders claims. His position was that even if the principle is to be preserved in relation to such claimants, the questionable nature of the justification for it means that it is appropriate for this court to stand back and ask afresh whether it can be justified as a principle to exclude otherwise valid claims made by a person who is a creditor of the company.[12]

Implications

The significance of such a long and controversial line of authorities being overturned cannot be overstated. In contrast with the line of authorities deriving from the principle of reflective loss over the last 40 years, the decision provides clear and narrow parameters for the application of reflective loss. It is both helpful to practitioners, and an apparent win for creditors, who no longer have to overcome the principle of reflective loss when recovering losses from third parties and potential fraudsters, simply by virtue of the fact that the debtor is a company. For example, as is the case in *Marex,* it will now be easier for claimants to bring claims against asset stripping shareholders and other third parties.

[12] [211]

About the Authors

Anthony Riem is recognised as 'stellar practitioner' and leading lawyer in fraud investigation and litigation, asset recovery, banking litigation and commercial litigation. Anthony has an established practice acting for banks in multi-million dollar litigation, often involving freezing orders in several jurisdictions. In addition, he has been instructed in many leading commercial litigation cases over the years, at both first instance and appellate levels. Anthony is a founding member and former Chairman of the Commercial Fraud Lawyers Association. He is also top ranked in Chambers, the Legal 500 and Who's Who Legal in fraud and asset recovery work in addition to being one of the English members of Fraudnet, the ICC global network of asset recovery specialists.

Catherine Eason is a civil litigator and advises clients on a range of complex issues and claims. Catherine has experience working on multi jurisdiction asset recovery and fraud cases, as well as enforcement proceedings and commercial contract claims.

Anthony Riem
Partner, PCB Litigation Solicitors

Email: ajr@pcblitigation.com
T: +44 (0) 7887 732 522

Catherine Eason
Senior Associate, PCB Litigation Solicitors

Email: ce@pcblitigation.com
T: +44 (0)20 7831 2691

PCB LITIGATION SOLICITORS

Using Bankruptcy Proceedings to Investigate and Combat Fraud

Joe Wielebinski & Matthias Kleinsasser

Abstract

As in the recent past, the current global economic downturn caused by the Covid-19 pandemic is likely to reveal widespread fraudulent conduct, requiring the need to pursue fraud claims and recover assets. Since transparency is integral to the U.S. bankruptcy process, a bankruptcy proceeding can be a useful tool to discover, investigate, and litigate fraudulent conduct. In this article, Joe Wielebinski and Matthias Kleinsasser of Winstead PC provide an overview of common bankruptcy discovery devices and causes of action available to professionals seeking to remedy fraudulent conduct. They also discuss why involuntary bankruptcies and Chapter 15 proceedings can prove useful in these circumstances.

1. Introduction

As Warren Buffett famously stated, "you only find out who is swimming naked when the tide goes out." Mr. Buffett's quotation is likely to prove apt yet again in light of the global economic downturn caused by Covid-19, particularly with regard to sectors such as the petroleum industry that are facing additional challenges beyond the pandemic. For professionals pursuing claims based on fraudulent conduct or attempting to recover fraudulently transferred assets, the U.S. bankruptcy laws and the attendant transparency of bankruptcy proceedings can prove to be a powerful tool. This article provides an overview of the bankruptcy process, including common discovery devices, causes of action, and other mechanisms available under American bankruptcy law for parties seeking to combat fraud.

2. Uncovering Fraud Using Bankruptcy Proceedings

Transparency is an integral feature of U.S. bankruptcy proceedings. A debtor that wishes to obtain the benefits of bankruptcy—*e.g.*, the breathing spell provided by the automatic stay and the exclusive right to propose and confirm a Chapter 11 plan—must provide creditors and the court

with extensive information under penalty of perjury regarding its assets, liabilities, pre-bankruptcy transfers of property, and other critical issues. These disclosure requirements can often be used by creditors and other parties to uncover fraud.

(1) Schedules and Statements of Financial Affairs. The documents required to be filed in the initial stages of a bankruptcy provide substantial information about the financial state of the debtor. Promptly after the bankruptcy case is commenced, the debtor must file a schedule of all assets and liabilities ('Schedules'), a statement of financial affairs ('SOFA'), a list of creditors, and other documents disclosing important information regarding assets, liabilities, transfers, creditors, and other matters.[1] For example, Schedules list all types of assets and separate creditors into categories (secured, priority unsecured, and general unsecured).[2] The SOFA requires a debtor to disclose information such as revenue for the debtor's current fiscal year and two preceding fiscal years, transfers of money or property that could be potentially clawed back (*e.g.*, transfers that benefitted insiders within one year of the petition date).[3] These documents must be signed by a representative of the debtor under penalty of perjury.[4] Courts have generally held that draft bankruptcy schedules and other documents intended for public filing are not protected by the attorney-client privilege or the work product doctrine, meaning that a party who suspects fraud on the part of the debtor may be able to obtain prior versions of these documents to compare to the filed version.[5]

(2) Rule 2004 Examinations. One discovery device commonly used to learn more about the debtor's financial affairs is an examination under Rule 2004 of the Federal Rules of Bankruptcy Procedure.[6] The scope of Rule 2004 is broad: a bankruptcy court may order examination of any person or entity to investigate, among other things, the debtor's acts, conduct, liabilities, and financial condition.[7] The examining party may request production of documents.[8] Rule 2004 examination requests are rarely denied. Given their broad scope, they are often referred to as "fishing expeditions" and are routinely used by trustees, creditors, statutory committees (e.g., committees of unsecured creditors), and other parties-in-interest to investigate a debtor and related parties.[9] If fraudulent conduct is suspected, a party should strongly consider applying for and conducting a Rule 2004 examination.

3. Combatting Fraud Once It Has Been Uncovered

The Bankruptcy Code provides multiple options for addressing fraudulent conduct once it has been uncovered:

---

[1] 11 U.S.C. § 521(a)(1)(B); Federal Rule of Bankruptcy Procedure ("FRBP") 1007.
[2] Official Forms have been issued for Schedules, SOFA, and other required filings, which are available at https://www.uscourts.gov/forms/bankruptcy-forms.
[3] The term "insider" is defined in 11 U.S.C. § 101 to include most persons and entities related to the debtor, such as partners, affiliates, and equity owners.
[4] FRBP 1008.
[5] *See, e.g.*, *United States v. Naegele*, 468 F. Supp.2d 165, 171-73 (D.D.C. 2007) (discussing inapplicability of these privileges to documents intended for public filing).
[6] FRBP 2004.
[7] FRBP 2004(a) and (b).
[8] FRCP 2004(c).
[9] *See In re Correra*, 589 B.R. 76, 108-09 (Bankr. N.D. Tex. 2018) (stating that a Rule 2004 examination's scope is "unfettered and broad" and "in the nature of a fishing expedition").

(1) Involuntary Bankruptcy Proceedings: One possible course of action for a creditor who believes someone is fraudulently dissipating assets is to place the person or entity in an involuntary bankruptcy proceeding. Section 303 of the Bankruptcy Code permits three or more creditors whose claims total at least $16,750 to file a bankruptcy petition against a debtor who is not generally paying debts as they become due.[10] If the debtor has fewer than 12 creditors (excluding creditors who are employees, insiders, and recipients of avoidable transfers), one or two creditors whose claims total at least $16,750 can file the involuntary petition. The petitioning creditors' claims must neither be contingent as to liability nor subject to bona fide dispute as to liability or amount.[11] If the debtor contests the involuntary filing, the court will hold a trial to determine if the requirements of Section 303 have been met. Involuntary bankruptcies are often quite expensive and should not be commenced lightly. If the bankruptcy petition is dismissed, the courts have the ability to award the debtor attorneys' fees, as well as actual damages and punitive damages if the bankruptcy was filed in bad faith.[12] But if creditors prevail, the bankruptcy should provide an opportunity to conduct significant discovery with respect to the debtor's conduct through a court-supervised process with significant penalties for a debtor who fails to adhere to the rules.

(2) Trustees and Examiners. Section 1104 of the Bankruptcy Code requires a court to appoint a trustee in a Chapter 11 case for "cause," such as fraud, dishonesty, incompetence, or gross mismanagement on the part of the debtor's management. The court may also appoint a trustee if appointment is in the best interests of creditors, equity security holders, and other interests of the estate.[13] Both pre- and post-bankruptcy conduct may serve as a basis to appoint a trustee,[14] though as a practical matter a court is less likely to appoint a trustee for pre-bankruptcy conduct if it does not rise to the level of fraud. If a trustee is appointed, the trustee is required to investigate the acts, conduct, assets, liabilities, and financial condition of the debtor[15] and is granted extensive powers by the Bankruptcy Code, including the power to recover assets and seek avoidance of improperly transferred property.[16]

Alternatively, the court can order appointment of an examiner if the court determines that the circumstances do not warrant appointment of a trustee.[17] An examiner generally is granted broad powers of investigation by the court but lacks a trustee's power to displace the debtor's management and file lawsuits on behalf of the debtor. Nevertheless, an examiner can serve an important role in uncovering fraud.

(3) Avoidance Actions and Other Estate-Owned Claims. The Bankruptcy Code allows a bankruptcy trustee to file several types of lawsuits (frequently referred to as avoidance actions) to

---

[10] 11 U.S.C. § 303. The minimum aggregate claim value is periodically adjusted upward for inflation. To the extent the petitioning creditors' claims are secured by property, the value of the claims must exceed the value of any lien on the property by at least $16,750. *Id.* § 303(b)(1).
[11] 11 U.S.C. § 303.
[12] 11 U.S.C. § 303(i).
[13] 11 U.S.C. § 1104(a)
[14] 11 U.S.C. § 1104(a)(1).
[15] 11 U.S.C. § 1106(a)(3).
[16] 11 U.S.C. §§ 544(b), 547, and 548.
[17] 11 U.S.C. § 1104(c). A court may appoint an examiner if appointment is in the best interests of creditors. The court must appoint an examiner upon request if the aggregate value of unsecured claims total at least $5 million (excluding claims for goods, services, and taxes and claims belonging to insiders).

recover property improperly transferred by the debtor. These actions include suits to recover preferential payments to creditors or insiders under Section 547, suits to recover pre-bankruptcy fraudulent transfers under Section 548, and suits to recover improper post-bankruptcy transfers under Section 549. In Chapter 11 cases, unless the court has appointed a trustee, the debtor's management continues to manage the debtor and operate its business, albeit with fiduciary obligations to creditors. In effect, the pre-bankruptcy debtor is transformed into an entity referred to as a "debtor-in-possession."[18]

Like a trustee, the debtor-in-possession has standing to prosecute causes of action owned by the bankruptcy estate, such as fraudulent transfer actions under Section 548 and breach of fiduciary duty claims against officers and directors.[19] As a practical matter, however, a debtor's management is unlikely to pursue claims based on their own bad acts. For this reason, many courts have held that an Official Committee of Unsecured Creditors can acquire standing to bring estate-owned claims on behalf of the creditor body upon a showing that colorable claims exist and that the debtor's management has unjustifiably refused to pursue them.[20] Some courts have held that an individual creditor may also acquire standing to pursue these claims.[21] A creditor who is aware of colorable estate-owned claims should strongly consider requesting that the Official Committee of Unsecured Creditors seek standing to pursue them, or, failing that, consider requesting the right to do so on its own. Of course, any recovery on avoidance actions or other estate-owned claims will benefit the unsecured creditor body as a whole, not the individual creditor.

One of the most useful avoidance actions when a debtor has improperly dissipated assets is the fraudulent transfer cause of action provided by Section 548. The statute allows for recovery of both actual and constructive fraudulent transfers. Actual fraudulent transfers are transfers of property made with actual intent to hinder, delay, or defraud a creditor.[22] Constructive fraudulent transfers are transfers of property made while the debtor was insolvent or undercapitalized and with respect to which the debtor did not receive reasonably equivalent value in return.[23] A creditor who acquires standing to bring a fraudulent transfer action may recover the property transferred, or, if the court so orders, the value of it, from a transferee, subject to certain defences.[24]

4. Bankruptcy Fraud and Other Criminal Matters

Chapter 9 of the federal criminal code, codified in Title 18 of the United States Code, covers crimes committed in connection with a bankruptcy proceeding.[25] While a detailed examination of bankruptcy crimes is beyond the scope of this article, it is worth noting that most bad acts committed in connection with a bankruptcy proceeding are federal crimes—e.g., fraudulently concealing assets in connection with a bankruptcy, knowingly making a false statement in a bankruptcy proceeding,

---

[18] 11 U.S.C. §§ 1107, 1108.
[19] 11 U.S.C. § 1107 (stating that a debtor-in-possession has most of the powers of a trustee).
[20] *See, e.g., In re Gibson Grp., Inc.*, 66 F.3d 1436, 1446 (6th Cir. 1995); *La. World Exposition v. Fed. Ins. Co.*, 858 F.2d 233, 247 (5th Cir. 1988).
[21] *See, e.g.*, *Gibson Grp.*, 66 F.3d at 1446.
[22] 11 U.S.C. § 548(a)(1)(A).
[23] Unlike actual fraudulent transfers, constructive fraudulent transfers do not require that the transfer be made with actual intent to hinder, delay, to defraud a creditor.
[24] 11 U.S.C. § 550(a).
[25] 18 U.S.C. §§ 151-158.

or filing a bankruptcy petition for the purpose of executing a scheme or artifice to defraud.[26] United States Attorneys have prosecuted numerous bankruptcy crimes, including several against high profile individuals, such as the baseball player Lenny Dykstra and the reality television stars Joe and Teresa Giudice.[27] A party with evidence that a bankruptcy debtor (or its management or affiliates) has engaged in fraudulent conduct may wish to consider raising these concerns with the United States Trustee (the branch of the U.S. Department of Justice charged with overseeing bankruptcies), the Federal Bureau of Investigation, or other regulators.[28]

5. Chapter 15 Bankruptcy as a Tool for Foreign Representatives

(1) Chapter 15 of the Bankruptcy Code addresses cross-border insolvencies and is based on UNCITRAL's Model Law on Cross-Border Insolvency.[29] A Chapter 15 bankruptcy proceeding is commenced by a "foreign representative" who files a petition for a U.S. bankruptcy court to recognize a "foreign proceeding"—in most cases, an insolvency proceeding pending in a foreign jurisdiction.[30] The bankruptcy court has authority to recognize the foreign proceeding as either a "foreign main proceeding," meaning that the foreign proceeding is pending in the country in which the debtor has its "center of main interests" ('COMI'), or, alternatively, as a "foreign nonmain proceeding" if the proceeding is pending in a country where the debtor has an "establishment" but not its COMI.[31] The bankruptcy court is authorized to order preliminary relief when a Chapter 15 proceeding is commenced, including entrusting the debtor's assets in the United States to an examiner.[32] If the bankruptcy court recognizes the foreign proceeding, it may grant additional relief such as suspending the right to transfer the debtor's assets and providing for the examination of witnesses under Rule 2004 of the Federal Rules of Bankruptcy Procedure.[33] Recognition of the foreign proceeding also provides the foreign representative with avoidance action powers available under applicable foreign law.[34] In determining whether to provide additional assistance to a foreign representative, the bankruptcy court should consider, among other things, prevention of preferential or fraudulent dispositions of the debtor's property.[35] Chapter 15 can serve as a potent tool for a trustee or other foreign representative investigating fraudulent conduct, particularly when assets are located in the United States.

---

[26] 18 U.S.C. §§ 151, 157.

[27] *See, e.g.*, Case No. 2:11-cr-00415-DDP, in the U.S. District Court for the Central District of California (Lenny Dykstra criminal proceeding); Case No. 2:13-cv-00495-ES, in the U.S. District Court for the District of New Jersey (Joe and Teresa Giudice criminal proceedings).

[28] Any such complaint should be made only if the party believes in good faith that the debtor or its principals have engaged in fraud and not as a means to gain an advantage in litigation. For example, most U.S. codes of professional conduct for attorneys prohibit an attorney from threatening criminal charges or participating in a criminal matter solely to gain an advantage in civil litigation. *See* Tex. Disp. R. Prof. Conduct 4.04(b).

[29] Chapter 15 was adopted in 2005 as part of the Bankruptcy Abuse Prevention and Consumer Protection Act, Pub. L. 109-8, 119 Stat. 23, enacted April 20, 2005.

[30] 11 U.S.C. §§ 1504, 1521.

[31] 11 U.S.C. § 1517.

[32] 11 U.S.C. § 1519(a)(2).

[33] 11 U.S.C. § 1521; *see also In re Platinum P'ners Value Arbitrage Fund L.P.*, 583 B.R. 803, 810-11 (Bankr. S.D.N.Y. 2018) (discussing applicability of Rule 2004 in Chapter 15 proceedings).

[34] *Tacon v. Petroquest Res. Inc. (In re Condor Ins. Ltd.)*, 601 F.3d 319, 323-29 (5th Cir. 2010). Avoidance actions under the Bankruptcy Code, such as Section 548 fraudulent transfer lawsuits, are available to a foreign representative only if a separate Chapter 7 or 11 proceeding is commenced. *Id.* at 323 (discussing 11 U.S.C. § 1523).

[35] 11 U.S.C. § 1507.

6. Potential Steps for Investigating Fraudulent Conduct or Pursuing Claims

Below is a list of potential steps which may be taken in connection with a bankruptcy proceeding by a party investigating fraudulent conduct, pursuing claims for fraud, or seeking to recover assets.

(1) U.S. Government resources: Often, the most difficult step in pursuing fraudulent conduct or recovering assets is determining what course of action best fits the situation. The resources available on the websites for the U.S. Department of Justice, U.S. Department of State, and other agencies are a good place to start.[36]

(2) Obtain qualified counsel: It goes without saying that obtaining qualified U.S. bankruptcy counsel is a must. The legal issues and discovery devices discussed above have complexities beyond the scope of this article. Qualified bankruptcy counsel can assist with developing and pursuing an effective strategy.

(3) Make use of the public nature of bankruptcy proceedings: As with most court proceedings in the United States, the vast majority of documents in a bankruptcy proceeding are available to the general public. If the party you are pursuing has filed for bankruptcy (or is involved in one), start by determining what information can be gleaned from documents such as Schedules and Statements of Financial Affairs.

(4) Pursue discovery: If further investigation is required, consider seeking a Rule 2004 examination of appropriate parties (not just the debtor) or request that the case Trustee or the Official Committee of Unsecured Creditors do so if a committee has been appointed. To the extent a party is aware of potential estate-owned claims against management or related parties, the party should bring those claims to the attention of the Creditors' Committee and/or the case Trustee.

(5) Commence a proceeding: A creditor pursuing a debtor who would be subject to jurisdiction in a U.S. bankruptcy court should consider filing an involuntary bankruptcy proceeding if the cost can be justified and two other creditors are interested in joining the petition. A foreign representative such as a foreign trustee should strongly consider seeking recognition of the foreign proceeding under Chapter 15 and pursuing injunctive relief, discovery under Rule 2004, or appointment of an examiner.

4. Conclusion

Many experts predict an increase in fraud as the economy suffers the continuing impacts of the Covid-19 pandemic. One of the most important means to combat fraud is through the insolvency regimes in the U.S. and elsewhere. Not only does the U.S. Bankruptcy Code provide a transparent process, but also the Code contains a variety of effective tools to discover, investigate and litigate fraudulent conduct.

---

[36] *See, e.g.*, U.S. Asset Recovery Tools & Procedures: A Practical Guide for International Cooperation (2017), *available at* https://2009-2017.state.gov/documents/organization/190690.pdf.

About the Authors

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. Consistently ranked by *Chambers USA* as a 'Leader in Their Field' since 2005, Joe is a frequent speaker and a prolific author on a broad range of topics involving corporate reorganization, insolvency, financial restructuring, fraud, asset recovery and cross-border insolvencies. Joe is the Executive Director *Emeritus* of ICC-FraudNet and member of its Advisory Board. He is a member of the International Bar Association, International Association for Asset Recovery, American Bankruptcy Institute, Turnaround Management Association and recently served on the Law360 Editorial Advisory Board.

Matthias Kleinsasser is a member of Winstead's Business Litigation, White-Collar Defense and Business Restructuring/Bankruptcy practice groups. He regularly represents officers, directors, and other clients involved in private securities litigation, as well as in investigations brought by regulatory agencies such as the Securities and Exchange Commission and the FDIC. Matthias diligently represents clients in almost any kind of contested matter, be it a state court receivership, class action, AAA arbitration, inverse condemnation suit, or other dispute. He also frequently advises firm transactional clients with respect to contract negotiations and business disputes, particularly in the technology and healthcare fields. Matthias has significant fraudulent transfer litigation experience. He has advised foreign clients on asset recovery procedures under US law and is a Contributor to the CDR Essential Intelligence publication on "Fraud, Asset Tracing & Recovery." He has also represented debtors, creditors, and trustees in virtually all aspects of business bankruptcy proceedings, including contested asset sales and debtor-in-possession financing.

Joe Wielebinski
Shareholder, Winstead Attorneys
T. 214.745.5210
E. jwielebinski@winstead.com

Matthias Kleinsasser
Of Counsel, Winstead Attorneys
T. 817.420.8281
E. mkleinsasser@winstead.com

WINSTEAD
ATTORNEYS

Collateral Damage: How Lenders Lose Billions on Fake Commodities and Forged Documents

Jingyi Li Blank & Ian Casewell

Diamonds aren't always forever, as a leading European bank discovered when its collateral stash of the world's most precious stone went missing. In China, a bank was sure all that glittered was gold, but found the billions in "bullion" they lent against was actually gold-plated copper.

Lenders are just as easily scammed over more pedestrian commodities like pig iron and liquor or, quite often, just paper – forged documents representing ownership of stock, real estate, ships, airplanes or automobiles.

One of history's most famous frauds involved a product on nearly every kitchen shelf, and landed a crucial investing win for the not-yet famous Warren Buffett. In the 1963 "Salad Oil Scandal," a consortium led by American Express lost the 2020 equivalent of $1.5 billion by lending against a giant New Jersey tank farm supposedly filled with soybean oil. When the borrower defaulted, lenders discovered their collateral was mostly seawater, with just a little salad oil floating on top, according to "The Great Salad Swindle" by Norman C. Miller.[1]

According to a November 2015 New York Times article, "American Express was far from blameless in the scandal. An anonymous tipster explained [the] swindle to the company in 1960, including [the] method for filling tanks with seawater except for a narrow chamber of oil positioned under the measuring hatch. The accusations were largely ignored, and the fraud grew tenfold over the following three years, until American Express ('AmEx') had guaranteed more soybean oil than actually existed in the entire country."[2]

Buffett, who famously said "be fearful when others are greedy, and be greedy when others are fearful," saw a buying opportunity when AmEx shares 'tanked' in the scandal.[3] He reportedly

[1] Miller, Norman C. *The Great Salad Oil Swindle*. Baltimore: Penguin Books, 1966.
[2] Gramm, Jeff. 2015. "Why Buffett's Salad Oil Magic May Not Repeat for Ackman." *The New York Times*, November 4. Accessed December 07, 2020. https://www.nytimes.com/2015/11/05/business/dealbook/why-buffetts-salad-oil-magic-may-not-repeat-for-ackman.html.
[3] Ibid.

invested 40 percent of partnership assets into the financial services giant, and in short, more than doubled their money, according to a May 2017 Motley Fool article.[4]

Bankers and debt owners today still face audacious fraudsters and are deploying ever more intensive due diligence measures to thwart collateral scams before they happen. If a fraud does occur, sophisticated investors speedily engage teams of experienced asset tracing detectives to recover the maximum amount possible.

I run the Hong Kong office of Mintz Group, providing due diligence and asset tracing services on every continent around the world. While I manage high stakes global investigations, I am not your typical private detective. My first career was in finance, making loans and structuring deals in risky commercial transactions. In other words, I know collateral, how it's managed, and what can happen when lenders aren't looking.

Opportunities for Fraud Fueled by Record Debt

Global debt surged to a record $258 trillion in the first quarter of 2020, and debt levels are continuing to rise, according to the Institute for International Finance ('IIF'). The IIF reported in July 2020 that the Q1 2020 debt-to-GDP ratio jumped by over 10 percentage points to 331 percent – a record high and the largest quarterly surge on record. As leverage levels rise globally, 'secured lending' is usually seen as the safest option because lenders have access to underlying collateral, especially when borrowers have poor or no credit history. However, the due diligence process for verifying this collateral and background checking of borrowers is fraught with challenges.

From Gold to Pig Iron to Liquor

In July 2020, Wuhan Kingold Jewelry Inc. ('Kingold'), a NASDAQ-listed jewelry maker, was accused of having passed off 83 tons of gilded copper as gold bars to obtain RMB 20 billion (approximately US$ 2.9 billion) in financing from at least 12 institutional lenders in China, according to a Caixin article from that time.[5] It could be China's largest loan scandal by value, according to the South China Morning Post.[6] It's odd no one noticed that the "gold bars" were so light; copper is less than half as dense as gold. Perhaps the people doing the due diligence were just a bit "dense" themselves.

In another form of gold fraud, a company may lease gold from one bank and use the borrowed gold as collateral to borrow from another financial institution. In 2014, the Chinese

---

[4] Wathen, Jordan. 2017. "1 Stock That Was Pivotal in Billionaire Warren Buffett's Career." *Motley Fool*. May 27. Accessed December 07, 2020. https://www.fool.com/investing/2017/05/27/1-stock-that-was-pivotal-in-billionaire-warren-buf.aspx.

[5] Wu, Yujian, Wu Hongyuran, Bai Yujie, and Han Wei. 2020. "Mystery of $2bn of loans backed by fake gold in China." *Caixin*, June 29. Accessed December 07, 2020. https://asia.nikkei.com/Spotlight/Caixin/Mystery-of-2bn-of-loans-backed-by-fake-gold-in-China.

[6] Ren, Daniel. 2020. "How Kingold Jewelry's fake gold bars slipped through scrutiny in one of China's biggest loan scams." *South China Morning Post*, July 07. Accessed December 07, 2020. https://www.scmp.com/business/companies/article/3092042/explainer-how-kingolds-fake-gold-bars-slipped-through-scrutiny.

National Audit Office reported that 25 Chinese companies had obtained more than RMB 94 billion (approximately US$ 15 billion) in loans over two years in this manner, according to a June 2014 Financial Times article.[7]

In the past, we have worked on fraud involving tens of thousands of tons of Brazilian pig iron – a key steelmaking ingredient – that had been pledged as collateral to a European-headquartered bank. Upon inspection, the bank discovered that bags of sand were substituted for the pig iron, and pursued legal action against the borrower.

Sometimes lenders continue to take risks on unusual collateral previously proven to be troublesome. In April 2020, a department store in China's Guizhou province pledged more than 160,000 bottles of Moutai liquor for a RMB 230 million (approximately US$ 34 million) loan from the Bank of Guiyang, according to a Sina article from that time.[8] So far, the 2020 loan is not known to be problematic, but in a well-known 2013 case, four Hangzhou province fraudsters were apprehended for taking about RMB 200 million (approximately US$ 33 million) in loans against more than 8,000 bottles of fake vintage Moutai, according to a December 2013 Sohu article.[9]

Alcoholic beverages provide attractive opportunities for counterfeiting. Moutai is China's 'national liquor' and its producer, Kweichow Moutai, is currently the world's most valuable spirits company, according to a June 2020 BBC article.[10] In 2010, a genuine bottle of vintage Moutai could retail for up to $4,400, while a fake could be produced for a fraction of this amount. There are also well-known cases of fraud with other alcoholic beverages such as wine.

Fake Collateral, Forged Documents

The use of fake commodities often goes hand-in-hand with forged documents to create the appearance of authenticity. In a well-known case in 2014, a Chinese metals company, Dezheng Resources, was caught using fake certificates and receipts for copper and aluminum at a warehouse in Qingdao. In fact, Dezheng duplicated those documents to pledge the same fake collateral to at least 13 banks, creating losses of over $3 billion, according to a December 2018 Reuters article.[11]

---

[7] Mitchell, Tom and Xan Rice. 2020. "China companies fake gold deals for $15bn loans, says auditor." *Financial Times*, June 26. Accessed December 07, 2020. https://www.ft.com/content/a5361796-fd20-11e3-8ca9-00144feab7de.

[8] Wang, Jiming 王基名. 2020. "Guizhou xingli baihuo 16 wan ping Maotai diya rongzi 2.3 yi yinhang yuangong cheng "tepi yewu"" 贵州星力百货16万瓶茅台抵押融资2.3亿 银行员工称"特批业务" [Guizhou Xingli Department Store mortgaged 160,000 bottles of Moutai for RMB 230 million; bank employee said it underwent a "special approval process"]. *Sina*, April 28. Accessed December 07, 2020. https://finance.sina.com.cn/roll/2020-04-28/doc-iirczymi8758146.shtml.

[9] Zhejiang Online-Qianjiang Evening News. 2013. "Nanzi yong 1400 xiang jia maotai zuo diya dao yinhang chenggong daikuan 2 yi yuan" 男子用1400箱假茅台做抵押到银行成功贷款2亿元 [Man successfully mortgaged 1,400 boxes of fake Moutai for RMB 200 million bank loan]. *Sohu*, December 26. Accessed December 07, 2020. https://business.sohu.com/20131226/n392423518.shtml.

[10] Harper, Justine. 2020. "Kweichow Moutai: 'Elite' alcohol brand is China's most valuable firm." *BBC*, June 30. Accessed December 07, 2020. https://www.bbc.com/news/business-53216320.

[11] Reuters Staff. 2018. "Qingdao metals scandal accused handed 23-year jail term." *Reuters*, December 10. Accessed December 07, 2020. https://fr.reuters.com/article/us-china-metals-fraud-idUSKBN1O91G8.

Companies facing financial trouble may also sell pledged collateral without the knowledge of their lenders, as with the recent case involving Hin Leong Trading. In early 2020, battered by Covid-19 and the sharp fall in global oil prices, the Singapore firm – formerly one of Asia's largest oil traders – was found to have covered up about $800 million in trading losses, and had sold oil inventory that it had pledged to banks as collateral, according to a June 2020 Business Times Singapore article.[12]

As of April 2020, Hin Leong owed approximately $4 billion to at least 23 banks, and had less than $200 million in oil inventory and cash, according to media reports. In August 2020, Hin Leong's founder, Lim Oon Kuin, was also charged for instigating an employee to forge a document stating that the company had transferred one million barrels of oil to another company; this document was used to secure a further $56 million in financing, according to a an August 2020 Straits Times article.[13]

Lenders Impacted, Opportunities Available

While the full extent of the fallout from the collapse of Hin Leong, and a number of other Singapore-based commodity traders like Hontop, Zenrock and Agritrade remains to be seen, lenders have curbed their exposure to commodity traders after a string of collapses and scandals globally, according to various press articles.[14] In a contrarian move in September 2020, Deutsche Bank announced plans to increase lending to commodity-trading firms in the Middle East, "even as other banks back away after a spate of defaults in the industry, to help double the size of its business in the region."[15] Clearly, when some investors retreat after a painful loss, others come in and eat their lunch.

Due Diligence as Competitive Advantage

Savvy lenders, investors, and insurers conduct background checks before they part with money. They conduct due diligence of the other party's business practices and reputation, verify authenticity of the commodities and documents provided in the transaction through inquiries with people relevant to the transaction, and conduct site visits. Most fraud takes place at the local levels so it is important to get on-the-ground intelligence. For example, in the Qingdao case, global lenders

[12] Lee, Marissa. 2020. "Hin Leong unlikely to be rehabilitated on its own: PwC." *Business Times Singapore*, June 24. Accessed December 07, 2020. https://www.businesstimes.com.sg/energy-commodities/hin-leong-unlikely-to-be-rehabilitated-on-its-own-pwc.

[13] Leong, Grace. 2020. "Hin Leong founder O.K. Lim charged with abetment of forgery for cheating, out on $3 million bail." *The Straits Times*, August 14. Accessed December 07, 2020. https://www.straitstimes.com/business/companies-markets/hin-leong-founder-ok-lim-charged-with-abetment-of-forgery-for-cheating.

[14] Meijer, Bart H. 2020. "ABN Amro exits trade, commodity finance in corporate bank shake-up." *Reuters*, August 12. Accessed December 07, 2020. https://www.livemint.com/companies/news/abn-amro-exits-trade-commodity-finance-in-wider-industry-shake-up-11597241554034.html .; Rajbhandari, Alexandre. 2020. "SocGen shuts S'pore trade commodity unit after Hin Leong." *Bloomberg*, July 31. Accessed December 07, 2020. https://www.bloomberg.com/news/articles/2020-07-31/socgen-shuts-singapore-trade-commodity-desk-after-hin-leong-hit .; Martin, Matthew. 2020. " Deutsche Bank Bucks Trend, Looks to Commodity Traders for Growth." *Bloomberg*, September 14. Accessed December 07, 2020. https://www.bloomberg.com/news/articles/2020-09-14/deutsche-bank-targets-commodity-finance-to-drive-mideast-growth.

[15] Martin, "Deutsche Bank Bucks Trend," 2020.

thought they were dealing with international storage facilitators, but these companies were in turn using local warehouse operators to store the metals. Thus, the corruption that resulted in the forged documents and missing metals likely occurred at the lowest levels, according to media coverage of the lawsuits filed after the fraud was uncovered.[16]

We began with diamonds and will end this article with a story that is still unfolding. A major European bank became frustrated with non-payment on a more than $300 million line of credit issued to a major diamond producer with global operations including in India, Belgium, Israel, Dubai, and Angola.

The borrower repeatedly failed to make payment and their most recent exchanges with the bank were caustic – "a complete breakdown of [the] relationship" to quote one of the parties involved.

Suspecting fraud, the bank held a board meeting, and engaged lawyers and investigators. They served the diamond producer's principal owner at his residence, then went to the firm's nearby headquarters to serve more papers and inspect the bank's primary collateral: numerous bags of diamonds worth hundreds of millions of dollars.

Once the firm's vault was open, the bankers expressed relief that the bags they expected to see were there. But their hopes were dashed when they opened the bags and found diamond dust – an industrial product of much, much lower value than the diamonds they were expecting.

The asset search is on. To be continued ...

[16] Home, Andy. 2014. "Qingdao scandal casts a long shadow over metal markets: Andy Home." *Reuters*, December 18. Accessed December 07, 2020. https://www.reuters.com/article/us-qingdao-metals-ahome/qingdao-scandal-casts-a-long-shadow-over-metal-markets-andy-home-idUSKBN0JW18620141218 .; Wragg, Eleanor. 2019. "Analysis: Legal paths for banks facing metals fraud scandals." *Global Trade Review*, August 02. Accessed December 07, 2020. https://www.gtreview.com/news/asia/analysis-legal-paths-for-banks-facing-metals-fraud-scandals/.

About the Authors

Jingyi Li Blank (李婧怡) is the partner of the Mintz Group Hong Kong office. She speaks native English and native Chinese, and specializes in investment support and asset tracing. Before joining Mintz Group, she worked in Deutsche Bank and HSBC's leveraged and structured debt practice for nine years and has a deep understanding of financial transactions and a wide network of contacts. She has supported numerous investment funds, multinational companies, and litigators in their asset recovery efforts linked to fraud, and has worked for stock exchanges and financial regulators in both the U.S. and Asia.

Ian Casewell is a Partner and heads the Mintz Group's London office. He specialises in providing investigative support on large-scale disputes and fraud matters. Ian co-heads the firm's international asset-tracing practice, which has been helping creditors enforce judgments in hundreds of cases over the past 20 years. His team is retained as lead investigators on some of the world's largest fraud, dispute and judgment enforcement matters. He represents governments, companies and individuals, assisting in the tracing and recovery of substantial funds.

Jingyi Li Blank
Partner
Mintz Group, Hong Kong
T. +852-3963-9530
E. jblank@mintzgroup.com

Ian Casewell
Partner
Mintz Group, London
T +44 (0)20 3137 7004
E. icasewell@mintzgroup.com

MINTZ GROUP

Part IV

Cybercrime, Cryptocurrencies and Technology Threats

Push Payment Fraud and the Liability of Banks

Joanelle O'Cleirigh

Abstract

In this article, Joanelle O'Cleirigh, a partner of Arthur Cox, Dublin, examines the rise of authorised push payment fraud and its impact on financial institutions. Authorised push payment fraud raises questions surrounding the potential liability of banks for losses incurred by victims. This article also considers the response of the courts to this new and sophisticated form of cyber-fraud in trying to formulate a practical remedy for the victim. These issues have not yet come before the Irish courts, but recent decisions of the English courts may give some guidance as to a possible approach in Ireland.

1. Introduction

With the rise of new financial technologies comes the inevitable challenge of new and different forms of fraud. Authorised push payments, where the customer essentially 'pushes' money to the receiver, are now a feature of our everyday lives. Authorised push payment fraud ('APP') involves the manipulation of consumers into making real-time payments to a bank account controlled by the fraudster. The fraud is characterised by the use of social engineering techniques involving impersonation. The habits of the consumer are often tracked or monitored by hacking into email and other systems. Spending patterns are identified and mimicked such that the push payment does not raise suspicion. The bank receives instructions and authorisation to send money to a particular account, thereby subverting the bank's fraud control systems.

Given the bank's role in sending the fraudulent payment from the consumer's bank account, APP raises significant questions surrounding the responsibilities of the bank in facilitating a practical remedy for the consumer and the potential liability of the bank for the losses incurred by the consumer. These issues have not yet come before an Irish court, but recent decisions of the English court may offer pragmatic solutions.

First, and of central importance in providing a remedy for APP, is the worldwide *Mareva* injunction deployed by the courts in Ireland and the UK. When met with cases of APP, English courts have innovated and expanded the remedy by relaxing the requirement to provide clear identification of the account-holder in applications for worldwide *Mareva* orders.

[1] The banks' role in this process is significant.

Second, regarding the potential liability of the bank, the approach of the English courts demonstrates that liability is not reduced in cases involving sophisticated fraud notwithstanding a lack of dishonesty on the part of the bank.[2]

2. A Growing Issue

Although social engineering scams such as APP are a growing global concern[3], the UK is one of the few countries to collate and publish data on APP. UK Finance have reported[4] that the total losses due to unauthorised fraud in the UK in 2019 amounted to £825 million. Of this, APP amounted to £455.8 million, inclusive of both personal and business fraud. This was an increase of £102 million on the previous year. There were 122,437 APP cases in 2019, up from 84,624 in 2018.[5]

The escalation of APP is reflected in the increased response by regulatory bodies in the UK. In 2016, the consumers' organisation *Which?* made a "super-complaint" to the Payment Systems Regulator (the 'PSR') regarding banking consumers' acute vulnerability to electronic fraud, in particular APP. The PSR issued a response stating there was insufficient evidence to warrant a change in the law. The response however acknowledged a problem and sought further evidence of the scale of the fraud.

Subsequently, the PSR introduced a Contingent Reimbursement Model Code for Authorised Push Payment Scams (the 'Code'). There is no equivalent system established in Ireland. The Code, which is voluntary, entered into force on the 28th of May 2019 and allows for the reimbursement of the consumer where the payment transaction meets certain criteria. It must be an authorised push payment. Crucially, the payment must also be made between UK bank accounts, such that if the monies are sent overseas, the reimbursement Code does not apply. On the date of the Code's entry into force, 8 payment service providers, representing 17 consumer brands and over 85% of authorised push payments, signed up to the Code. Between May and December 2019, losses

---

[1] *CMOC Sales & Marketing Limited v Persons Unknown & Ors* [2018] EWHC 2230 (Comm).
[2] *Singularis v Daiwa* [2019] 3 WLR 997.
[3] See Europol, *2019 Internet Organised Crime Threat Assessment,* at 40 in which Europol identified Business Email Compromise as a constantly evolving threat and a crucial priority for Member States and the private industry; see also Federal Bureau of Investigations, '*Business Email Compromise The $26 Billion Scam'* (*Public Service Announcement*, 10 September 2019) https://www.ic3.gov/media/2019/190910.aspx#fn2 accessed 1 October 2020, in which the FBI noted that between May 2018 and July 2019, there was a 100% increase in global exposed losses due to Business Email Compromise.
[4] UK Finance, 'Fraud – The Facts 2020: The Definitive Overview of Payment Industry Fraud' (2020) available at: Fraud - The Facts 2020
[5] Ibid, p. 45.

as a result of APP amounted to £101 million. Of this, £41 million was returned to consumers.[6] The Code was recently extended to December 2020.

3. Practical Remedies in the Courts

Worldwide Mareva Injunctions

Through push payments, the defrauded monies are often sent to numerous bank accounts in different jurisdictions at the touch of a button. Consequently, tracing the assets and identifying the wrongdoers proves extremely difficult. Once described as one of the law's "nuclear weapons",[7] the worldwide *Mareva* injunction will take centre-stage in combating the threat posed to consumers by APP.

A unique aspect of *Mareva* injunctions is that, at a practical level, third-party banks are so often relied upon for their enforcement. This ensures the effectiveness of the remedy as, from the viewpoint of banks, they would have "*nothing to gain and all to lose*" by resisting a *Mareva* order of the court.[8] It is well-established in Ireland that the courts have jurisdiction to grant, as an equitable remedy, a worldwide *Mareva* injunction should the justice of the case so require. Referring to the English position set down in *Derby & Co. Ltd v Weldon (Nos. 3 and 4)*[9], Costello J in *Deutsche Bank v Murtagh* clearly stated that:

"*[I]n my opinion the court has jurisdiction to restrain the dissipation of extra-territorial assets where such an order is warranted by the facts. The basis on which a Mareva injunction is granted is to ensure that a defendant does not take action designed to frustrate subsequent orders of the court. It is well established in England that a Mareva injunction may extend to foreign assets and I believe that the Irish courts have a similar power in order to avoid the frustration of subsequent orders it may make.*"[10]

This position was recently reaffirmed by the Irish High Court in *Trafalgar Developments Ltd. v Mazepin.*[11] Relying on *Murtagh*, Barniville J held that *Mareva* style injunctive relief can:

"*in appropriate cases and where the circumstances warrant it, extend to assets located outside the jurisdiction.*"[12]

It is also settled law in Ireland that the courts can grant ancillary orders for the purpose of effecting the *Mareva* injunction. In *Irish Bank Resolution Corporation Ltd. v Quinn,*[13] citing the English Court of Appeal in *House of Spring Gardens Ltd v Waite,*[14] Kelly J was satisfied that:

"*the court has inherent jurisdiction to ensure that injunctions granted by it are effective. In the case of the Mareva type injunction this may involve orders of discovery, disclosure, the answering of interrogatories or the production of a deponent for cross examination.*"[15]

---

[6] Ibid, p. 46.
[7] *Bank Millat v Nikpour* [1985] FSR 87 (Donaldson LJ).
[8] Thomas Courtney, 'Civil Arrest and Injunction to Restrain An Absconding Defendant From Leaving the Jurisdiction Part 1' (1990) *8 Irish Law Times* 200.
[9] [1989] 2 WLR 412.
[10] *Deutsche Bank v Murtagh* [1995] 1 ILRM 381, at p. 388. This was subsequently affirmed and applied by Sullivan J in *Bennett Enterprises Inc v Lipton* [1999] 2 IR 221.
[11] [2019] IEHC 7.
[12] [2019] IEHC 7, at para. 103.
[13] [2013] IEHC 388.
[14] [1985] FSR 173.
[15] [2013] IEHC 388, at para. 29.

The granting of such ancillary orders in combination with the principal *Mareva* injunction is particularly important where the nature of the fraud is APP. It facilitates the swift identification and investigation of the wrongdoer such that the stolen assets can be traced and sequestered.

Innovation in the UK

In the UK, APP has presented unique and novel challenges before the courts. Typically, APP involves an anonymous fraudster imitating the actions of the true consumer. This feature of APP presents courts with an unidentifiable wrongdoer, banks with an apparently genuine payment request, and ultimately results in a defrauded customer with no means of compensation. The UK courts have responded and developed innovative and practical solutions to combat this new and sophisticated cyber-fraud, such as expanding the worldwide *Mareva* injunction as an equitable remedy and extending the duty of care imposed on financial institutions.

In its landmark decision in *CMOC Sales & Marketing Limited v Persons Unknown*[16], the English High Court granted the first known worldwide *Mareva* injunction against "Persons Unknown". CMOC Sales & Marketing Limited ("CMOC") was the victim of a sophisticated hacking into one of its directors' email accounts. The hackers sent requests to CMOC's bank, purportedly from the director, directing it to make payments totalling in excess of US$8 million to accounts in 50 banks across 19 countries. The Court in *CMOC* held that there were strong reasons to allow for the granting of worldwide freezing orders against unidentified parties:

"First, the orders can act as a "springboard" for ancillary reliefs which would never have been possible without initially notifying the banks to freeze the accounts and prevent the dissipation of the relevant assets."

"Second, critical information is obtained from banks as a result of the granting of an ancillary disclosure order, particularly the identity of the bank account-holders. This is of crucial importance as it facilitates the investigation of the parties, the tracing of the assets and the implementation of measures to recover the stolen property".[17]

In this case, the orders helped CMOC to identify the perpetrators. CMOC was subsequently able to get various court orders requiring the defendants to repay the monies stolen or received by them (approximately US$1 million) in addition to damages for the loss suffered.

The decision in *CMOC* was recently followed by the English High Court in *World Proteins Kft v Persons Unknown.*[18] The fraudster, impersonating the company's supplier, sent emails requesting payments of £500,000 and £1.5 million from the company within a chain of previous legitimate emails from the supplier. Citing *CMOC*, the Court granted the interim orders against persons unknown, obliging the bank to freeze the account and make an ancillary disclosure of key information in relation to the account-holder.

In addition to the expansion of injunctive relief to unknown persons, it will be of interest that they have also allowed for more innovative and alternative methods of service on defendants in these cases. In *CMOC*, the Court upheld service on the defendants and banks through email, Facebook

[16] [2018] EWHC 2230 (Comm).
[17] [2018] EWHC 2230 (Comm) at paras. 183-184.
[18] [2019] EWHC 1146.

Messenger, WhatsApp and later through the establishment of an online virtual data room.[19] Similarly, in the decision of *Clarkson Plc v. Person(s) Unknown*[20], the English High Court accepted the service of the interim court order and other application documents by way of a specified email address.[21]

It is evident, flowing from this approach, that the responsibility of banks will likely be quite extensive. Not only will banks be obliged to step in and freeze assets against unknown parties on a global scale, but further will be obliged to gather and furnish account-holders' information facilitating their identification and investigation.

There has been no Irish case on the granting of a *Mareva* injunction against unknown persons. However, based on the law in Ireland in relation to worldwide *Mareva* injunctions, an Irish decision in line with *CMOC* would provide a practical remedy for consumers in response to the growing threat of APP, raising real and practical considerations for banks.

Liability of Banks in APP Cases

A worldwide *Mareva* order is effective in circumstances in which the misappropriated funds can be traced to identifiable bank accounts. However, frequently, the funds are distributed quickly through numerous bank accounts in numerous jurisdictions, and are ultimately untraceable, leaving no avenue of compensation open to the defrauded victim. The recent UK Supreme Court decision of *Singularis v Daiwa*[22] provides a remedy for defrauded customers, imposing liability for fraudulent payments on the customer's bank if the customer can demonstrate that the bank was negligent in accepting the customer's instructions.

The case concerned a fraudulent request by an officer of the company to transfer funds out of funds held for the company by Daiwa. Daiwa was unaware that the payments constituted a misappropriation of Singularis' funds. The Supreme Court upheld the judgment of the Chancery division of the English High Court in finding that there was a breach of the *Quincecare*[23] duty of care on the part of the bank by failing to detect and prevent the fraudulent transaction. The *Quincecare* duty of care, as defined by Steyn J, states that:

"a banker must refrain from executing an order if and for so long as the banker is 'put on inquiry' in the sense that he has reasonable grounds (although not necessarily proof) for believing that the order is an attempt to misappropriate the funds of the company"[24].

The foregoing was cited with approval by Herbert J. in the Irish case of *Razaq v Allied Irish Banks plc*.[25] In *Singlaris,* the Supreme Court stated that:

[19] [2018] EWHC 2230 (Comm) at para. 51.
[20] [2018] EWHC 417 (QB).
[21] [2018] EWHC 417 (QB), at para. 11.
[22] [2018] 1 WLR 2777.
[23] *Barclays Bank Plc v Quincecare Ltd* [1992] 4 All ER 363.
[24] Ibid at para 179.
[25] [2009] IEHC 176.

"Daiwa should have realised that something suspicious was going on and suspended payment until it had made reasonable enquiries to satisfy itself that the payments were properly to be made."[26]

The Court reasoned that as a result of such enquiries, Daiwa would have undoubtedly concluded that the payments were suspicious. Although, the facts of *Singularis* concern a fraud committed by an officer of the company, the decision paves the way for the *Quincecare* duty to be invoked in relation to APP.

The impact of this decision is two-fold:

(i) Firstly, it provides that negligent banks may be responsible for compensating their customers even if payments were authorised by the customer in apparently routine instructions. Unhelpfully, it does not provide guidance as to when the bank is on notice of a suspicious transfer or what enquiries should be made before executing the transfer.

(ii) Secondly, it places liability on the customer's bank, not the recipient bank. The Code provides an alternative to this approach, acknowledging that situations arise in which the recipient bank must bear some responsibility. Pursuant to the Code, the sending and receiving banks agree how to allocate victim reimbursement.[27]

In practical terms, the extension of the *Quincecare* duty of care by the Supreme Court will require financial institutions to have in place proper safeguards and governance structures to identify, and prevent, fraudulent transfers. This is likely to become increasingly important with the continuous increase in online transfers and the sophistication of the tactics employed by cyber criminals. UK authorities are sometimes cited with approval in Irish courts and given the advancement of this area of law in the UK, it is likely that the Irish courts may take a similar approach.

4. Concluding Thoughts

The decisions in *CMOC* and *Singularis* highlight the willingness of courts to provide remedies to victims of cyber-fraud, and raise considerations for the role and responsibilities of banks. However, the decisions provide little clear practical guidance to banks involved in such cases. In particular, the decision in *Singularis* presents banks with a conflict between their duty to give effect to customer instructions and the duty of care as stipulated in *Quincecare.* The increase in APP in the UK is undoubtedly reflected in Ireland, and Irish courts and banks will closely monitor the regulatory and legal developments across the water.

The author would like to thank Laragh Lee and Eamonn Butler for their assistance with this article.

[26] *Singularis v Daiwa* [2019] 3 WLR 997, at para. 39.
[27] Contingent Reimbursement Model Code, at 15.

About the Author

Joanelle O'Cleirigh is a Partner in the Litigation, Dispute Resolution and Investigation Group at Arthur Cox. Joanelle has over twenty years' experience in investigations, inquiries and commercial litigation matters including advising on white collar crime matters and fraud and asset recovery cases.

Joanelle O'Cleirigh
Partner

Arthur Cox
W. www.arthurcox.com
E. joanelle.ocleirigh@arthurcox.com

ARTHUR COX

Case Study of the Coincheck Cryptocurrency Hack: a Major Japanese Cryptocurrency Exchange Lost "NEM" Worth USD 530 million due to Cyber-Attack

Hiroyuki Kanae & Hidetaka Miyake

Abstract

In this article Hiroyuki Kanae and Hidetaka Miyake discuss, by reference to a case study, a significant cyber-attack in Japan. The case discussed in this article is the biggest cyber-attack of a cryptocurrency exchange to date and new challenges and developments are observed in Japan to address various issues raised in the case. This article touches upon some of the new challenges and developments in the areas of asset recovery, criminal enforcement, regulatory actions and class action. Although enormous efforts have been made by government agencies and other stakeholders, no criminal enforcement or regulatory or class action has been brought against the cyber-attackers thus far and no asset has been recovered from them. In the meantime, the Japanese authorities strengthened the regulations on cryptocurrency exchange business in response to this incident. This case illustrates the importance of criminal enforcement and asset recovery for growth of a new market of cryptocurrency business.

Case Summary

Coincheck, Inc. ("Coincheck"), one of Japan's leading cryptocurrency exchange service providers, suffered a cyber-attack on 26 January 2018. During this attack, a cryptocurrency called "NEM" which was held by Coincheck was illegally transferred outside the company by the attackers. As a result, Coincheck's customer assets suddenly disappeared. Anonymous hackers appeared to have spread malware and penetrated Coincheck's internal network via employees' infected personal computers. The value of stolen "NEM" was 54.7 billion yen at that time. This case is the biggest cyber-attack of a cryptocurrency exchange to date, surpassing the US$460 million attack on Mt. Gox in 2014. It is generally acknowledged that this huge loss of customer assets was caused not by a problem with the NEM cryptocurrency itself, but rather by Coincheck's weak security system. Coincheck's major security weakness was that it did not manage customer assets in an off-line "Cold Wallet". As a result, about 260,000 customers' NEM wallets were hit by the cyber-attack, which

forced the Japanese government and financial regulators to fundamentally strengthen their regulations on cryptocurrency exchanges and related security protocols.

Asset Recovery

It was an extremely difficult proposition to track down and recover the stolen cryptocurrency. In February 2018, a website suddenly appeared in a group of anonymous sites that require special software to access called the "Dark Web". This site offered to exchange bitcoin and other cryptocurrencies for NEM at a discount relative to the normal market price. This website is believed by experts to have been set up by the hackers involved in the attack on Coincheck. Accordingly, many people made purchases from that website, and it is likely that almost all of stolen NEM was exchanged for other currencies by March 2018.

In the meantime, Coincheck announced on 27 January 2018 that it intended to compensate its customers for their stolen NEM. As a result, Coincheck eventually paid a total of 46 billion yen on 12 March 2018 to its customers who held NEM as of 26 January 2018, taking into account the decline in NEM's market value over that period.

Criminal Enforcement

The Tokyo Metropolitan Police Department (the 'TMPD') set up a special investigation team of around one hundred highly experienced cybercrime specialists within the Cyber Crimes Division to investigate the Coincheck case. These criminal investigators have been trying to charge the hackers involved in the attack on Coincheck with the violation of the Unauthorized Computer Access Law. However, thus far no criminal charges have been brought against the attackers by the public prosecutor.

In April 2020, as a result of the investigation by the above-mentioned Cyber Crimes Division of the TMPD, the public prosecutor of the Tokyo District Public Prosecutors Office brought criminal charges against two Japanese suspects for accepting criminal proceeds, as prohibited under the Act of Punishment of Organized Crimes, Control of Crime Proceeds and Other Matters (the 'Organized Crime Punishment Act'). According to the indictment from the public prosecutor and other information, the two suspects are alleged to have purchased large quantities of NEM between February and March 2018 at low prices through an automated trading program that made many high-speed transactions in a short period of time. The accused allegedly knew that the NEM that they were purchasing was stolen from Coincheck. The two suspects also allegedly exchanged the stolen NEM for another cryptocurrency and, as a result, made a profit of billions of yen. One of the two suspects has pleaded not guilty and the criminal trials of both accused are still ongoing.

Over the course of the investigation into the Coincheck case, criminal investigators used a new tool to freeze the assets of one of the above-mentioned criminal suspects. In response to the TMPD's request, the Tokyo District Court issued, on 30 March 2020, a protective order for confiscation against a company managed by one of those criminal suspects. This order was issued prior to the public prosecutor's indictment under the Organized Crime Punishment Act. This was the first time a pretrial protective order for confiscation under the Organized Crime Punishment Act was issued in Japan. Any property obtained through criminal acts or obtained as remuneration for

criminal acts may be subject to confiscation and, if a protective order for confiscation is issued, criminal suspects will be prevented from disposing of such property even before the public prosecutor's indictment and the commencement of a criminal trial.

Regulatory Actions

Due to the fact that the legal status of Bitcoin and other cryptocurrencies were unclear under Japanese law, and that there were no clear regulations on cryptocurrency exchange service providers, the Japan Financial Services Agency (the 'JFSA') introduced the amended Payment Services Act, which came into force in April 2017. The amended Payment Services Act introduced a new registration requirement for "cryptocurrency exchange service providers". However, as a transitional measure, service providers that had been operating before the enactment of the amended Payment Services Act were categorized as "deemed cryptocurrency exchange service providers". These deemed providers were allowed to continue their business subject to the new regulations if they applied for registration. At the time of the incident on 26 January 2018, Coincheck was still undergoing the process of completing their registration. Therefore, the company was still a deemed cryptocurrency exchange service provider.

In response to the incident, financial regulators immediately issued a business improvement order against Coincheck on 29 January 2018. In addition, the JFSA commenced an on-site inspection of Coincheck on 2 February 2018. On 8 March 2018, another business improvement order was issued against Coincheck, calling for the fundamental restructuring of its management system and strategy, as well as other measures to ensure proper business operations. In addition, the JFSA also issued administrative orders on 2 February 2018 against other service providers to submit reports on their risk management systems.

As of 12 September 2018, the financial regulators issued business suspension orders and business improvement orders against ten deemed cryptocurrency exchange service providers, as well as seven registered cryptocurrency exchange service providers. As a result, more than a dozen deemed cryptocurrency exchange service providers withdrew their applications for registration. The Coincheck case had a significant negative impact on the cryptocurrency exchange market in Japan, which was otherwise expected to grow under the new regulations. Eventually, Coincheck became a wholly owned subsidiary of Monex Group, a major online financial institution, in April 2018 and subsequently completed its registration as a cryptocurrency exchange service provider in January 2019.

The JFSA further amended the Payment Services Act and other legislation to strengthen regulations surrounding cryptocurrency. These new amended regulations came into force in May 2020 and (among other measures) changed the legal term from "virtual currency/cryptocurrency" to "crypto asset".

Class action

Between 26 and 27 February 2018, Coincheck customers filed a series of lawsuits seeking the return of their cryptocurrency assets. As of the 27 of February 2018, a total of 144 Coincheck customers had filed lawsuits. Since then, the number of plaintiffs has gradually increased, and it is

estimated (case records are not disclosed to outside non-interested parties in Japan) that nearly 200 plaintiffs have filed lawsuits.

These civil suits have sought damages for (i) the difference between the Coincheck's discretionary compensation and the price of NEM at the time of the cyber-attack, and (ii) the amount that the price of cryptocurrencies deposited by customers in Coincheck had declined by during the suspension of trading of the assets (including 11 virtual currencies other than NEM). Losses to customers were caused by the decline in the value of NEM and many other virtual currencies because Coincheck suspended trading of all virtual currencies for a period of time after the NEM cyber-attack. The main issue in the case is whether the difference between the NEM price at the time of the attack and the amount that Coincheck voluntarily compensated can be awarded as damages.

In these lawsuits, the plaintiffs (Coincheck's customers) sought, from the Toyko District Court, a document production order on a report submitted to the FSA by the defendant (Coincheck). The plaintiffs intend to use this report to prove that the defendant was negligent while in custody of the plaintiffs' virtual currencies. In response, on November 11 2019, the Tokyo District Court issued a ruling to "dismiss the petition". This meant that no order was issued against Coincheck to produce reports and other documents filed with the JFSA and the Kanto Local Finance Bureau.

In its decision, although the Court accepted the plaintiff's arguments that (1) Coincheck is the holder of the documents (i.e. the reports, etc. submitted to the JFSA, etc.), (2) the subject documents had been identified by the plaintiffs, and (3) there is a need to examine the evidence, the Court concluded that the contents of the reports, etc. would "undermine the relationship of trust between the supervisory authorities and Coincheck, thereby impeding the fair and smooth operation of public services" if they were to be made public. Accordingly, the Court did not order Coincheck to produce the reports, etc. submitted to the JFSA, etc. pursuant to Article 220, item (iv), (b) of the Code of Civil Procedure.

On November 15, 2019, the plaintiffs' counsel filed an immediate appeal (i.e. procedures for filing an objection) against the Tokyo District Court's decision. As a result, the Tokyo High Court will determine whether or not to order the production of documents. Unlike in the United States and elsewhere, there is no system for discovery in Japanese civil suits. Therefore, it is extremely difficult for the plaintiffs to present evidence in court and, accordingly, prove the defendant's negligence. Since more than two years have passed since the filing of these lawsuits, it is expected that the outcome of these civil suits will be unfavorable for the plaintiffs.

Conclusion

In conclusion, after almost three years of asset recovery efforts against the cyber-attackers involving Coincheck, one of the major cryptocurrency exchange service providers, they have faced numerous obstacles due to the difficulty of identification of such attackers and cross-border impediments. Further, although more than one hundred cybercrime specialists of the TMPD have investigated the incident and the cyber-attackers, law enforcement authorities could not identify the attackers and recover the stolen cryptocurrencies. While the JFSA issued a number of rules and guidelines for the strict enforcement on the security requirements on the cryptocurrency exchange service providers, once the cyber-attackers hacked the network sysem and conveyed the cryptoassets into other locations, it is almost impossible to trace and recover such assets from the attackers. Therefore, for

now the cryptocurrency exchange service providers should make every exertion on the strict security measures and the training of their employees to avoid any loopholes for cyber-attackers.

About the Authors

Hiroyuki Kanae has more than 30 years' experience in the cross-border litigation. 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 Pacific and Europe. He has represented trustees in bankruptcy proceedings in Japan, in pursuing successful asset recovery in the United States.

Hidetaka Miyake is one of the leading lawyers in the fields of government investigations and crisis management in Japan. By leveraging his background as a former public prosecutor, a former senior investigator at the Securities and Exchange Surveillance Commission and a former forensic senior manager of a Big Four accounting firm, he focuses on handling internal or independent investigations for listed companies to address complex accounting frauds. He also handles crisis management for financial institutions and criminal defense for non-Japanese clients. Since joining Anderson Mori & Tomotsune in 2017, he has been involved in accounting fraud investigations for more than 12 Japanese listed companies.

Hiroyuki Kanae
Anderson Mori & Tomotsune
T. +81-3-6775-1011
E. hiroyuki.kanae@amt-law.com

Hidetaka Miyake
Anderson Mori & Tomotsune
T. +81-3-6775-1121
E.hidetaka.miyake@amt-law.com

ANDERSON MŌRI & TOMOTSUNE

Do You Value Your Assets?

Rami Tamam & Gilad Cohen

Abstract

These are special times that requires special means. In this article Rami Tamam and Gilad Cohen of Tamam, Rotenberg, Bar & Co discuss the fragility of asset-keeping in these times, and the need of a swift response in order to recover goods stolen in cases of cyber fraud.

1. Introduction

"Do you value your assets?" Nearly all of us, when asked that question, may think immediately of assets such as our home, our stocks, our pension, or our vehicle. Perhaps some think of their factory, machines, and stock. Few consider their organization's data assets. This review endeavours to clarify that for every business (not exclusively hi-tech organizations) their most important asset is their data. Data can be many things: a customer list or suppliers, patents, thinking, production procedures. But it is much more. Assets include personal, even embarrassing information; information that can present an organization or those heading it in a less-than-positive light. Every factory, safe or vehicle, has a key and alarm to keep it safe. Are your data assets protected by a similar mechanism? The answer is usually: no.

2. A Case Study

The following example, paraphrased and anonymized accordingly, illustrates this point. John heads a communications organization that is currently in the midst of a merger and acquisition process with a much larger international organization. John is preparing for the challenges and opportunities this merger may encompass, including reducing local headquarters to expand the company and thus make it international. Unfortunately, John's morning took a totally different turn. An hour into his morning, John gets a call from a journalist asking for comment about claims that the company acted in a conflict of interest in a foreign country while bribing the local company not to take part in any tenders in the country. John then is contacted by the country's largest cable provider claiming John's company has been postponing his cheques for 120 days. "This is it", he

says. I am through with your company. An hour later, the CEO of said international organization calls to inquire whether, during the due diligence process, John's company concealed the fact that their last five bids for government tenders have been rejected on grounds of inadequate corporate governance?

This outcome was the result of a company worker pairing with a relatively low-level hacker. Using basic tools, such as social engineering and accessing organizational emails, they attempted to prevent the merger process which may have harmed the worker's position. Original documents were planted into company servers, and by simply editing the names of their payment destinations, falsely presented decision-makers with these 'transfers'. These documents were sent to journalists via the organizational email of one of the organization's CEOs, complete with a list of facts that fitted the attachments. Through another organizational email, belonging to an accountant, they sent messages to all suppliers stating that "due to a financial crisis, the company regretfully is pending all payment". The fake tender proposals were sent to the purchasing organization, hidden among authentic documents. These could all have been prevented by asset charting: strategic files, customer list, supplier list, encrypted data, etc.

In this case, the organization acted quickly. The organization's remaining assets were secured and mapped, while relevant evidence was collected. An in-depth forensic inspection of all computers and email correspondences revealed that this was an 'inside job'. The material was collected as part of a legal process of legal risk hedging and considering further action, including pressing charges against the hackers, and involving the police. Thus, the inspection was kept entirely secret. Meanwhile, company workers were equipped with the right messages and all interfaces through which the fictitious correspondences were fixed.

Not every company would had taken this course of action. Admitting to such an infiltration may be considered a sign of weakness, and as such may typically be dealt with discretely. Besides, most organizations do not possess the technological and legal tools to deal with a cyber crisis. Not only does the secretive handling of this situation ironically prevent exposition, but also there is a limited timeframe during which the company can still respond. Once the time is up, the company remains without solution and substantially harmed. Many cases include a subsequent call for help due to a ransom demand following a simple email sent to the company. These emails contain a virus which locks all files on the computer a day or two later. All data on such an organization's network would now be encrypted, with the perpetrator holding the keys to it. Companies tend to try and solve these cases on their own. They try bargaining with the offender or recreate the data either independently or by hiring a computer support service. These tactics only enhance the infiltration, usually leading to the loss of vast amounts of financial and corporate data. The financial loss is usually immense.

Nowadays, in circumstances of Covid-19 and the necessity of remote working, many organizations are being attacked by various hackers using the "man in the email" technique. This is when they remain in the organizational email network after hacking into it. Organization workers contact a legitimate party they know but, after sending, someone intercepts their email altering its content and sending it back to the sender. These workers are oblivious to the fact that someone is faking both sides of the correspondence, or of the illegitimate content they have received. In these cases, hundreds of thousands, sometimes even millions of dollars are stolen by someone who is fooling both sides. Only after the money has already been transferred from one account to the other, yet the receiving side has not received its share, do they start asking questions. Both sides are puzzled,

and such a case can harm business connections. However, once they contact each other and share copies of their correspondence, they realize that they were victims of a well-crafted scheme. Needless to say, the money has long gone by then.

3. Concluding Thoughts

We recently handled cases in which a quick response to the threat was crucial to preventing the transfer. In some cases, we intercepted transfers and, collaborating with the police and the global network of lawyers to which we belong, successfully intercepted the entire sum. In other cases, some of the sum was already withdrawn while the rest of it was successfully intercepted. The legal technological interface in these cases is a tiebreaker when facing these adversaries. In such circumstances, we urge you to seek expert advice that will hedge the risk, stop the data leakage, and will initiate the money tracing and recovery.

Our firm dealt with cases like these during the past year, and since COVID19 got into our lives on March 2020 the cases became more frequent, and the perpetrators more sophisticated and bold. It looks like the incident first and swift response was the game changer, and in the cases in which we were called few days from the incident we managed to recover the funds (or some of it). Please don't hesitate to call.

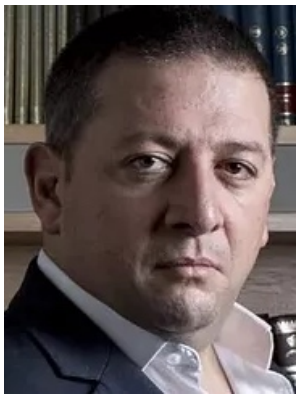
About the Authors

Rami Tamam holds a Bachelor's Degree in Law from Tel Aviv University, Master's Degree in Law from Bar Ilan University, and has been accepted to the Israel Bar Association many years ago. Rami served as senior officer in the Israel Police in various positions in Lahav 433, spearheading investigations as joint task force commander with the Police, the State Attorney's Office, the Tax Authority and the Prohibition on Money Laundering Authority. As Unit Leader, Rami led investigations of financial cases, public corruption, cyber and online gambling that were the focus of public interest in Israel and abroad, including investigations of prime ministers, ministers and other officials, the Ashdod Port case and international crime organizations. These investigations were supported by the State Attorney, the Attorney General and various senior prosecutors. Rami directed precedent regulatory processes, including blocking illegal gambling websites and "blacklists" of bank accounts. Rami provides his extensive knowledge, experience and skills to public and private sector clients. Rami is a guest lecturer in the Hebrew University and a part-time teacher at Sapir Academic College and the Ono Academic City, specializing in money laundering and cybercrime. Rami recently finished composing a joint project with senior economists from Harvard and MIT: the Parliamentary Investigation Committee Report on Credit Extension to Tycoons - Kabel Committee. He had previously chaired the Meuhedet HMO investigation committee and provided opinions on corporate office holders offenses in various companies in the Israeli market.

Gilad Cohen was in the Air Force for 8 years in various positions. He spent another 8 years in the Israel Police in the field of anti-money laundering and counter-terrorist finance. In recent years, he was the CEO of the Israeli Defense Forum (HLS & CYBER Forum) which includes 195 senior CEOs of the defense industry in Israel. He serves as a senior technological and strategic consultant to companies and startups in Israel and abroad, as well as a mentor on behalf of Sigma Lab and the Israeli Export Institute. Gilad has participated in many ventures in fundraising companies (Investor Forum GSEK), a company for renewable energy through wind turbines (Windbazz), a company for the separation of voices in the field of security (Insight Acostics)

Rami Tamam
Partner
Tamam, Rotenberg, Bar & Co
Aviv Tower. 52 Floor, Jabotinsky 7, Ramat Gan, Israel

T. +972(50)4003544
E. rami@rtco-law.com



Gilad Cohen

E. gilad@insightacoustics.com

Tamam, Rotenberg, Bar & Co.
LAW OFFICE

The Approach of Polish Law to Cryptocurrencies – selected issues

Joanna Bogdańska

Abstract

With the increasing interest in cryptocurrencies and their wider use, not only in everyday life, but also in criminal activities, this paper examines the approach of Polish law to Cryptocurrencies. Joanna Bogdańska, Attorney-at-Law at KW Kruk and Partners, Warsaw, Poland, questions whether the existing principles of criminal law meet the new realities of cryptocurrencies? This paper presents a summary of the most interesting and ever-developing aspects concerning cryptocurrencies in the context of Polish criminal law. Due to the complexity of this contemporary subject, this paper examines the foundational doubts as to the nature of the cryptocurrencies in relation to traditional criminal law institutions.

General information

So far in Poland, no dedicated regulations have been created concerning the functioning of cryptocurrencies and crypto exchanges. However, the use of cryptocurrencies in Poland should be considered as fully legal on the basis on the statement of the Ministry of Development and Finance.[1] On the basis of analysis from Polish experts, it states that there is currently no justification for working on a separate piece of legislation on blockchain technology or cryptocurrencies. It was also stressed that their application is fully legal in Poland. It was also declared that as part of further work, a sub-group dedicated strictly to legal issues is to prepare proposals for changes in current regulations or directions of changes in current regulations that constitute unjustified barriers to specific applications of blockchain technology. Further work will be devoted to new constructions and legal regulations that unblock or sanction the use of blockchain technology by sector (block) and identification of barriers to the development of the crypto currencies market in Poland and proposals for their elimination.

[1] Response of the Minister for Development and Finance to the question (interpellation) No. 6655 by Member of Parliament Mirosław Suchoń on cryptocurrencies of November 2, 2016

While there is still a lack of information on the definition of cryptocurrencies in Polish legislation, trade and revenue generation from the sale of cryptocurrencies are already covered by Polish tax law. Under Polish tax law, cryptocurrencies are treated as property rights. Therefore, the provisions of tax laws apply to virtual currency trading. Individuals obtaining revenue from the exchange of cryptocurrencies into a domestic or foreign currency obtain taxable revenue in the same way as revenue from property rights, as defined in Article 18 of the Personal Income Tax Act of 26 July 1991.

Cryptocurrency as a subject of the offence

As the cryptocurrency itself does not appear in Polish laws, first of all its nature should be defined in criminal law on the basis of existing definitions. Below is an overview of the offences with regard to their subject matter, and thus the fulfilment of the constituent elements of the offences.

Cryptocurrency as movable item, money and means of payment

In accordance to article 115 paragraph 3 of Criminal Code, a movable item or object includes Polish or foreign currency, or another means of payment, and a document entitling the holder to a sum of money or setting out an obligation to pay capital, interest, a share in the profits or an interest in a company.

Certainly, a cryptocurrency is neither Polish nor foreign currency. But can a cryptocurrency be considered as electronic currency? According to the statutory definition, electronic money is the monetary value stored electronically, including magnetically, issued, with the obligation to redeem it, for payment transactions, accepted by entities other than the issuer of electronic money alone.

Cryptocurrency is presently accepted by various economic operators, so it can be considered to be accepted by operators other than the issuer alone. It can also be considered that as part of the cyber world, cryptocurrency is stored electronically – for example in a virtual user wallet. However cryptocurrency does not represent a specific monetary value. A digital record of its value depends on how much other trading participants are able to pay for it. And although there are similarities between cryptocurrencies and electronic currency, under the Polish laws cryptocurrency may not be treated as electronic currency.

How about the last part of definition, i.e. another means of payment? From the study of criminal law, it follows that the means of payment should enable its independent use in trade and fulfil analogous functions of circulating money, i.e. the ability of its use instead of money will be a manifestation of this ability. What is more, this feature should be generally accepted. There is no doubt that cryptocurrency has a payment function and although it cannot, in itself, be a means of redemption and a substitute for money in this regard, by agreement the parties can give it that value. However, the main disadvantage associated with cryptocurrency as another means of payment is their lack of universal acceptability, as it is only recognized and perceived as measurable value by some entities. It is widely recognized in the science of criminal law that it is precisely because of the lack of universality that the crypto is not a means of payment[2].

[2] See also: Judgment of Voivodship Administrative Court seat in Poznań of 19 December 2018. (file No. I SA/Po 802/18)

Taking this into consideration, cryptocurrency may not be directly a subject of offences such as the offence of counterfeiting, or the placing of counterfeit or forged money on the market.

Cryptocurrency as a property right / asset

Cryptocurrency as a digital record, to which participants in trade give a certain intentional value, cannot itself be a property right. However cryptocurrency can undoubtedly be an object of property law. This is primarily a matter of relative property law (e.g. debts), but also absolute property law. As a dematerialized entity, it cannot theoretically be an object of property. However, even in the doctrine of civil law, one may encounter the position that having cryptocurrency at one's disposal is a beneficial factual situation and as a such is legally protected interest.

The criminal understanding of the term 'property law' allows the 'owner' of cryptocurrency to be protected as well. This is due to the fact that although cryptocurrency itself is not a property law an action aimed at a cryptographer can be considered as affecting the beneficial, factual situation of the victim, characterized by property. Thus it may indirectly be the object of offences that contain an infringement of property.

Undoubtedly, the features of a cryptocurrency indicate its character of subjective rights closely related to the economic interest of the entitled person, connected with his or her property and characterized by two basic features: transferability (can be traded) and possession of a specific property value. As such, a violation of the right to dispose of the cryptocurrency or deprivation of its possessions causing damage to the injured party's property may constitute a punishable act. By adopting the above definition, a cryptocurrency may be the subject of such offences as extortion, fraud as well as money laundering, crimes against creditors, misappropriation.

Cryptocurrencies & security of enforcement of judgements

If the accused is charged with an offence liable to a fine, monetary performance, forfeiture, compensatory measure, or financial return to the aggrieved party or another entity – the enforcement of the judgment may be secured *ex officio* on the property of the accused if there is a justified concern that without such a security the enforcement of the judgment will be impossible or significantly hindered. As was mentioned above, cryptocurrencies are property right and falls within the concept of the property, and as such may be the object of property security. However, the difficulty may be caused by the way in which the cryptocurrencies are actually secured. On the one hand, the digital recording should be secured in such a place that it is not exposed to unwanted transfers. On the other hand, the prosecutor or court must have an access to them, in the event of a fall in security or to make them available for enforcement purposes.

It seems that the only way to effectively secure the crypto-asset from their undesirable regulation is for the prosecutor/court to create a wallet. Since the creation of such a wallet and the transfer of the relevant crypto-asset to it requires expertise, it will be necessary to use expert assistance to establish such collateral. This may result in the ineffectiveness of such a security because practically it takes time for the court and the prosecutor to appoint an expert and physically hand him over even a fragment of the file. Another difficulty in establishing such security may be the legal requirement to determine the amount of the object of security. The cryptocurrencies rates are

different on each stock exchange and are also highly changeable. Unfortunately, doctrine and judicature have not yet developed any practice in this area.
On the basis of the above, it should be concluded that in the current legal status, a cryptographer cannot be considered as money or any means of payment. On the other hand, a cryptographer may be the object of offences in which there is an element of financial benefit.

Summary

It should be expected that the subject of cryptocurrencies will increasingly enter the area of criminal law. From year to year, the number of crimes carried out with the use of cryptocurrencies grows. This is especially so in the area of money laundering. It seems at this stage that there is no need to drastically change the provisions of Polish substantive criminal law. The current law provides protection for users of cryptocurrencies. The protection of interests is also realized by constantly evolving regulations related to the prevention of money laundering, which are successively introduced into the Polish legal order. With time, a natural evolution of criminal proceedings is also expected, towards enabling the law enforcement authorities to better control the flow of cryptocurrencies or implement security measures, as well as forfeitures of cryptocurrencies which are the subject of criminality. Also in this case, the law must follow the development of technology.

About the Author

Joanna Bogdańska is an Attorney-at-Law at KW Kruk and Partners, Warsaw, Poland.
Her practice deals with the current service of business entities and corporate service of commercial law companies, including current strategic consulting, mergers and acquisitions, investment and negotiation processes. She has extensive experience in conducting criminal proceedings (white-collar crimes) and asset recovery processes.

Joanna Bogdańska
KW Kruk and Partners Law Firm

14 Bł. Ładysława z Gielniowa Street
02-066 Warsaw, Poland
E. Joanna.bogdanska@legalkw.pl
T. +48601830633

KW KRUK AND PARTNERS
LAW FIRM

Failing to Prevent – Virtual Asset Service Providers' Liability for Abuse of Traded Cryptoassets

Chris Stears

National Competent Authorities are policing an ever-broadening regulatory perimeter for traded cryptoassets. The fault lines hitherto demarcated by the more traditional, regulated, market intermediaries, have moved to capture "virtual asset service providers" ('VASPs').

This short briefing considers this new regulated market facilitator and highlights a few points on the efficacy of the new standards in the context of virtual asset ('VA') transfers, as VASPs face a clear and present 'failing to prevent' risk.

On 21 June 2019, the Financial Action Task Force ('FATF') issued an Interpretative Note to Recommendation 15 on New Technologies (INR. 15) containing binding international standards on the prevention of misuse of VA's for money laundering. INR. 15, while clarifying a number of important definitional issues, notably requires countries to create a regulatory perimeter (whether by licence or registration) around otherwise unregulated entities such as VASPs. VASPs are required to implement the full gamut of FATF Recommendations, including measures to monitor transactions and report suspicion, in line with other entities subject to AML/CTF regulation.
VASPs are defined in the FATF Glossary as:
"any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

(i) exchange between virtual assets and fiat currencies;
(ii) exchange between one or more forms of virtual assets;
(iii) transfer of virtual assets;
(iv) safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and
(v) participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset."

Clearly this would capture financial institutions and other market actors already regulated and carrying on such activities. For the purpose of this note however, the focus is on those VASPs not within the traditional regulatory purview. With respect to the UK

[1] this would include cryptoassets exchange providers, Peer to Peer Providers, Initial Coin Offerings or Initial Exchange Offerings, as well as Custodian Wallet Providers[2] - not all of whom will already be regulated to provide financial services. This is a most critical component of the regulatory intervention in VA markets if such markets and market participants are to be effectively protected.

As the FATF Guidance[3] accompanying INR.15 refers, the VA space has evolved to include a range of new products and services that do not always intersect with, and provide a gateway to and from, the traditional regulated financial system[4]. Rather, transactions can exist entirely within the virtual ecosystem, with a significant reduction in transparency and increased obfuscation of financial flows and attendant risk of fraud and market manipulation.[5]

Looking specifically at the secondary market, VASPs who are 'actively' facilitating VA activity are charged, it would appear, with a *de facto* obligation, to monitor for suspicious transactions, alongside other mitigating duties; and with equal emphasis to those placed on their more sophisticated colleagues. The preventative measures set out in FATF Recommendations 10 to 21 all apply to VASPs.

Where VAs are traded, VASPs must conduct ongoing monitoring to determine whether the transaction in relation to which VASP actively facilitates is consistent with the VASP's understanding of the customer and the nature and purpose of the relationship. Enhanced monitoring will likely serve as the benchmark and not the exception for the crypto markets (certainly absent intermediary financial institutions and fiat conversion flow). However, striking a defensible risk-based approach to monitoring for suspicious activity/transactions (with respect to both AML/CTF and market abuse regimes) will prove challenging. The regulatory risk, never mind financial crime risk, is palpable. Take, for instance, the FATF Guidance Note which state that VASPs should extend enhanced monitoring activity "beyond the immediate transaction between the VASP or its customer or counterparty"[6]. The Guidance does not elaborate on what that might entail.

Recommendation 16, for example, places an obligation on the VASP to obtain, hold and transmit required originator and beneficiary information, immediately and securely, when conducting VA transfers. Is that always going to be possible? Indeed, VASPs must go further and have in place systems and controls to take freezing actions and prohibit transactions with designated persons/entities, where necessary. Again, will this always be possible? It is accepted that technology/software will be crucial here. The VA transfer's underlying Distributed Ledger

---

[1] See the Money Laundering and Terrorist Financing (Amendment) Regulations 2019 No. 1511, amending the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017; implementing the EU's 5th Money Laundering Directive

[2] Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, Regulations 14A(1) and (2)

[3] FATF, 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' (June 2019)

[4] Ibid at para 3.

[5] Ibid at para 4. It is noted that the FATF Guidance focuses on the AML/CTF risks in transfers or conversions of Vas and, while there will be a clear read over to anti-fraud or anti-market manipulation issues, the Guidance does not address these risks specifically.

[6] FATF Guidance n.5 at para 184

Technology transaction protocol, for example, will likely need to contain code, or an existing linked platform, to capture the necessary information. But we need to also acknowledge the operational, legal and potential market risk where the transaction is effected through the use of smart contracts, auto-executing; preventing ex-ante validation of transaction/beneficiary information for regulatory compliance purposes. The value of any freezing action could well be undermined. The secure transmission of verified information, accessible by those facilitating the transaction, at the right time in the transaction flow, is critical to Recommendation 16's objectives; and by extension to Recommendation 20, which requires VASPs to have the ability to flag for further analysis any unusual or suspicious movements of funds or transactions.

VASP exposure to financial crime risks may extend beyond brokerage, custodial or agency services. VASPs engaging in market making, or trading as principal in back-to-back transactions with customers, may also be exposed, say, as a result of the use of smart contracts. Quite aside from facilitator liabilities discussed above, the subject cryptoasset could be at risk of manipulation. The UK Jurisdiction Taskforce (UKJT)'s legal statement on cryptoassets and smart contracts (the Statement)[7] elucidates a number of issues in this regard. Key among which is that cryptoassets are to be treated in principle as property and that smart contracts are capable of satisfying the requirements for a binding contract under English law – a 'private key', for example, could be used to 'sign' the contract or the source code (where it is of sufficient specificity) may satisfy an 'in writing' requirement.

Therefore, it is possible that were a VASP to own a VA pursuant to a smart contract, but by some nefarious act, the VA is manipulated, lost or destroyed, then the VASP would suffer loss and may still have to perform its obligations to an end customer. Anonymity in this situation would not be a bar to the binding nature of the smart contract. The asset – at risk of manipulation in this context – is, as the Statement notes, the combination of the public and private keys, the distributed ledger data and the relevant system rules that provide the exclusive ability to update or spend transaction data (emphasis added). The owner of the cryptoasset is the "person who has acquired control of a private key by some lawful means."[8] A VASP may do so as a principal or may do so while acting as a custodian or intermediary. It follows therefore that where the cryptoasset is property, proprietary rights will arise unless there is a 'special legal reason to disqualify them'. This is significant in the context of tracing or recovering the asset that has been subject to fraud, theft or breach of trust. The VASP, for instance, may find itself subject to the establishment of a Quistclose or constructive trust or liable in restitution to its customer.

Anonymity remains a significant barrier to any successful tracing claim and, of course, with respect to the ability of VASPs, acting as intermediaries, to capture party/transaction information for the purposes of regulatory compliance. As the European Parliament noted in its July 2018 study of cryptocurrencies and blockchain[9], anonymity prevents transactions from being adequately monitored for fraud & market abuse risk and tax evasion, and facilitates money laundering. It will,

[7] The LawTech Delivery Panel, UK Jurisdiction Taskforce, 'legal statement on cryptoassets and smart contracts' (November 2019).
[8] Ibid at para 43.
[9] European Parliament, Study on 'Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion' July 2019

however, take time for market practice to mature and for technologies to be developed that address the anonymity issue and enable VASPs to comply with their market surveillance obligations.

Indeed, it is of some relief to VASPs that, following consultation on the implementation of the 5MLD, the UK has not, for time being, legislated to oblige the capture, holding and transmission of required originator and beneficiary information, immediately and securely, when conducting cryptoassets transfers.[10] The delay, it is intended, will provide time for VASPs to develop compliance solutions. Such solutions are most likely to be developed (or owned) by VASP's more sophisticated financial institutions and payments counterparts, leaving VASPs somewhat hostage to market development and access to accepted technologies.

While the regulatory net has rightly be cast wide to encompass the activities of VASPs, the roll-out and enforcement of the above-mentioned secondary market surveillance obligations should be staged to align with the ability of VASPs to comply.

VASPs can expect all regulatory authorities in scope of the, almost inevitably, cross-jurisdictional transaction, to co-ordinate supervisory efforts when policing VA transfer activity.[11] However, co-operation in the fight against financial crime associated with VAs, it is expected, will also extend to peer-to-peer information exchange (subject to any impediment at national level), such as that related to "blacklisted wallet addresses", enabling effective screening by VASPs as part of their due diligence activities. Any arrangement for the exchange between private counterparties of market integrity-related data received pursuant to otherwise private transactions would most likely require clear regulatory direction, if not a legislative framework analogous to the issues surrounding market access to SAR intelligence.

The extension of AML/CTF, anti-fraud and market abuse obligations to VASPs is unquestionably necessary. However, aside from the virtuosity of a regulatory stick, VASPs will want to protect themselves from legal and regulatory risk where, by dint of a VA's characteristics, market or beneficiary opacity, or the transfer/execution mechanisms, illicit activity prevails despite best efforts. NCA's supervisory and enforcement approaches will be front and centre in striking the right balance and protecting the integrity of virtual asset exchanges/secondary markets. It's very much a 'watch this [virtual] space'.

[10] See HM Treasury, 'Transposition of the Fifth Money Laundering Directive: response to the consultation', January 2020, para 2.24

[11] Subject to prevailing national data protection and privacy rules. See FATF, 'Guidance for Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers', June 2019

About the Author

Chris Stears is a Solicitor, General Counsel, Legal Consultant and Academic. He is a Visiting Lecturer in Financial Law and Compliance at BPP University Law School, and an Honorary Visiting Fellow, Faculty of Finance, Centre for Banking Research at Cass Business School. He is an Editorial Board member of the Company Lawyer journal (Sweet & Maxwell), and is the former founding member and research director of CCP Research Foundation. Chris serves as a Legal Consultant to DLA Piper and has spent time as a Visiting Scholar at the Law Commission of England and Wales, the G. Levin College of Law, University of Florida, and as a Senior Research Associate at the London School of Economics. He is a prolific writer and his academic research interests focuses on all aspects of financial market regulation, compliance and risk relating to financial crime – with particular emphasis on institutions, ESG legal risk due diligence and corporate finance. He is co-author of the book *Legal and Conduct Risk in the Financial Markets* (2018, Oxford University Press).

Chris Stears LL.B, LL.M, PDIC, Ch.FSCI, FRSA
Director, BisonCove

E. cstears@bisoncove.com

Covid-19 and its Impact on Fighting Fraud and Financial Crime

Dr Dominic Thomas-James

Abstract

In this article, Dr Dominic Thomas-James examines the impact of the global Covid-19 health pandemic on the fight against fraud and financial crime. He provides an overview of how fraud risks have increased due to, and as a result of, Covid-19 including in the cyber-space. He further considers the impact that the pandemic continues to have on global initiatives to fight fraud and economic crime – including the inevitable, yet problematic, delays of momentum-driven monitoring and review processes.

Background

Of economic crime's many impacts on society, business and institutions, its ability to threaten public finance – and, by extension, public services – is one of its most concerning aspects. In a time of a global health pandemic, people and countries are at their most vulnerable. Covid-19 has created an environment of overrun public health efforts, limited financial relief, increased unemployment, and disrupted education. The credit bubble is expanding, public services are overrun, and the justice system – in particular the courts – are dealing with a mounting backlog of cases. That is not to mention the countless injuries and thousands of deaths, and broader social costs, caused by this indiscriminate virus.

Fraud & Covid-19

It is the above backdrop which paves the way for a landscape of 'dangerous opportunity' in terms of financial crime. The environment is one in which perpetrators prey on the fears and vulnerabilities exacerbated by Covid-19. 'Adaptability' of fraudsters is something that has been acknowledged by international law enforcement agencies during this time.[1] Indeed, mainstream criminological explanations of crime often point to 'opportunity as one of crime's underlying cause.

[1] See, for example: Interpol (14 April 2020) 'Unmasked: International Covid-19 Fraud Exposed'.

Applying the 'Routine Activity' approach[2] to explaining crime, Covid-19 has created a perfect 'chemistry' for fraud.[3] The very nature of self-isolating and working remotely means that fraudsters can now more easily target our innate desire for the kind of human, social and professional interaction Covid-19 has largely prohibited. Combined with a climate of fear, it is a suitable backdrop for the old-fashioned confidence trick.

During the pandemic there has been a sharp increase in online frauds including cyber-threats, hacking, identity theft, phishing scams via emails and impersonation attacks, high-pressure selling of products and services (many Covid-19-inspired relating to health, debt, benefits and employment) and attacks that compromise business and other email accounts.[4] Attacks are not solely conducted by individual perpetrators, but are often the enterprise of organised criminal gangs. Interpol recently emphasised that during the pandemic, impersonation offences had significantly increased whereby unsuspecting victims would be solicited by criminals impersonating medical workers – for the purpose of fraudulently persuading them to part with money in order to settle bills for healthcare provided to relatives. Given how far-reaching the pandemic has been, and how close to home it has manifested for so many, this particular example indicates contextual adaptability and an air of believability from the part of the victim. This can be sharply contrasted with many of the poorly-drafted email phishing attempts such as those advising that you have inherited a fortune from someone in an overseas country, and need to provide bank details immediately for the transfer.

A significant area of ongoing concern, particularly in light of the unpredictability of national or regional lockdowns, is in the area of financial relief. There have been significant reports of misdirection or misappropriation of public and private sector relief schemes. One which has been affected is the furlough scheme in the U.K. – a government relief package subsidising 80% of workers' wages during lockdowns and other restricted periods.[5] In the U.K. alone, Her Majesty's Revenue and Customs estimate that currently £3.5 billion worth of claims under the government's furlough scheme were fraudulent or paid erroneously.[6] Examples of fraudulent claims in this regard may include requesting one's workforce to work normal hours yet, secretively and unbeknown to them, claiming furlough on their behalf in order to fraudulently obtain 80% of their salaries. Or, it could involve inflating company details at the application stage about the size of one's workforce. According to Adams-Prassl et al (2020), the prohibition of working while subject to the furlough scheme was "routinely ignored".[7] Enforcement authorities in the U.K. are reviewing presently some 27,000 cases in which fraud or error is suspected. The U.K. National Audit Office has initially assessed that over half of those which are fraudulent were perpetrated by organised criminal gangs posing as legitimate business. The furlough scheme was, however, widely accepted to be prone to fraudulent abuse based on the size of the financial packages available and the speed at which they were necessarily integrated into the economy to try and save businesses and livelihoods.

---

[2] This approach suggests that crime can be explained by reference to the following factors being present: a suitable perpetrator, a suitable target, and lack of a guardian against the crime taking place.
[3] See Felson, M. (1998) *Crime and Everyday Life* (2nd ed) Thousand Oaks, CA: Pine Forge Press.
[4] Financial Action Task Force (2020) Covid-19 Related Money Laundering and Terrorist Financing Risks and Policy Responses.
[5] For background, see: HM Government (2020) Coronavirus Job Retention Scheme: Claim for your Employees Wages', [2].
[6] Financial Times (7 September 2020) 'HMRC says fraud and error on furlough schemes could total £3.5bn', available at: https://www.ft.com/content/22f78e4a-8e24-4189-9983-3a1f95788340.
[7] Adams-Prassl, A., Boneva, T., Golin, M., and Rauh, C. (2020) 'Furloughing', *Cambridge Working Papers in Economics* 2079, [1].

Elsewhere, the U.S. Treasury reported that fraudsters are soliciting people while impersonating government workers. This is for the purpose of trying to elicit banking information from unsuspecting victims to assist them with tax rebates and other financial relief. Of course, related to these types of fraud are the more familiar pressure-selling operations and boiler-rooms, through which confidence is deployed to persuade the unsuspecting victim to part with their savings for the promise of investment returns. The landscape is such that relief schemes are constantly discussed in the news media, as well as the backdrop of rising debt and unemployment caused by the pandemic giving rise to people looking for some type of 'hope', which is where the pressure-selling methods of organised fraud take root and are most effective.

In this context, the Charities Commission in the U.K. reported that fraudulent charity operations are also on the rise, particularly insider fraud due to the economic hardship faced by employees who may abuse their position of trust (i.e. if tasked with fund-raising or administering, receiving or distributing donations) to make personal gain. Charities have also been the subject of the cyber-fraud context during Covid-19, whereby impersonation attacks have been seen in relation to monies which never actually reach the charitable destination the doner intended.[8] For example, email scams trying to fraudulently elicit donations for fake charitable causes to assist the National Health Services or volunteer organisations. If these examples demonstrate one thing, then it is the innovation of fraudsters. Criminal gangs operating an organised boiler-room type fraud scheme to convince a vulnerable person to donate money to a healthcare charity during a time of a global pandemic is greatly assisted by the fact that the weaknesses of the healthcare system are constantly being highlighted to us by governments and the media. There have been cases whereby fraudsters have falsely convinced unsuspecting victims that they can provide the vaccine or other medication quicker, for huge premiums.

The International Fight Against Fraud – and Covid-19's impact

Given the increase in various types of fraud, a word now on some of the global frameworks which exist to combat it and the impact Covid-19 is having on their momentum. The virus has exposed the fragility of the global fight against economic crime. The Financial Action Task Force ('FATF'), the unparalleled standard-setter for anti-money laundering and counter-terrorism financing standards, conceded early during the lockdown periods in 2020 that its typical activities of on-site visits, ongoing reviews and monitoring initiatives could not take place in the context of Covid-19. This was due to the restrictions in movement, but also the burdens placed on countries due to the pandemic – implying, at least, that implementing recommendations on AML/CFT compliance from previous mutual evaluation reports may, understandably, not assume its ordinary place on a given government's priority list. Essentially, and for the FATF process to not only fulfil its remit, but effect positive change in member countries reviewed, they would need longer to comply with the recommendations following previous reviews ahead of subsequent ones. A good example are National Risk Assessments for money laundering and terrorism – which are one of the ways countries can positively engage in the FATF process between reviews and identify risks not only in these two areas, but across the spectrum of financial and related sectors. Many of these kinds of initiatives are resource-intense and require active input from multiple stakeholders in society across

[8] The Charity Commission (UK) (19 October 2020) Press Release: 'Watchdog warns charities and the public to protect themselves against fraudsters amid pandemic'.

public, private and third sectors. As such, deadlines have been perhaps unsurprisingly extended by FATF for members to engage with the requirements for follow-up and monitoring processes.[9] Some deadlines have been extended to as far away as 2022.

As emphasised, this is perhaps unsurprising. However, it should be of concern given the implication that momentum is a collateral feature. Many developing jurisdictions have faced significant challenges implementing sophisticated international financial crime standards. However, as has been seen in jurisdictions like the Turks and Caicos Islands for example, momentum has played a critical role not only in compliance and engagement with international standards, but also how this has assisted, and translated to, institutional and legal development more broadly. For a jurisdiction who effectively lost its sovereignty over allegations of Ministerial corruption and money laundering little over a decade ago, it is reassuring to note proactive regional engagement with the Caribbean FATF, commission of a multi-stakeholder AML/CFT National Risk Assessment, establishment of various public sector accountability mechanisms such as registers of interest, and the adoption of integrity as a learning feature of educational curricula. All this demonstrates the cruciality of a momentum-driven approach in developing mechanisms to tackle financial crime. Delays in monitoring, while perhaps inevitable, represent a concern that these important issues (particularly in the case of those countries on an upward developmental trajectory) may be side-lined, or resources withdrawn or directed elsewhere. There has however been some good news in this regard, with momentum appearing to have been maintained in some jurisdictions – such as the Bahamas who recently graduated from FATF's greylist in December 2020.

Concluding thoughts

It is fundamentally concerning that Covid-19 has not only presented an opportunity for bad actors to innovate during these uncertain times, but also that momentum is being affected in key areas of the global fight against this type of acquisitive misconduct. In the case of international monitoring and peer-review evaluation, the inevitable delays are concerning. Covid-19 provides criminals not only with a vulnerable environment in which they can capitalise, but one whereby oversight measures may be protracted, resources cut, and progress in implementing economic crime standards side-lined. This is particularly concerning in the context of developing jurisdictions whose compliance with FATF standards is constantly subject to various bars and challenges. Momentum (or, at times, the lack thereof) is inarguably a hallmark of their compliance records to date. It is therefore concerning to consider the impact of loss of momentum, given the peer-review process has become the international best practice for evaluating compliance with global standards as they evolve.

[9] FATF (1 April 2020) Statement by FAFT President: Covid-19 and measures to combat illicit financing'.

About the Author

Dr Dominic Thomas-James serves as the Editor of the inaugural FraudNet Global Report. He is presently the Course Director of the International Development programme at the University of Cambridge Institute of Continuing Education, a member of the Cambridge Centre for Criminal Justice (CCCJ), and is a Global Justice Fellow at Yale University. His research interests include economic crime, financial regulation, international and offshore financial centres. Dominic earned his Ph.D. and M.Phil. from Queens' College, Cambridge. He serves as a Secretariat Member of the Annual International Symposium on Economic Crime at Jesus College, Cambridge. He lectures widely and is frequently invited to speak at conferences and forums internationally. Dominic's written work is regularly published in peer-reviewed journals and he is the author of the forthcoming book *Offshore Financial Centres and the Law: Suspect Wealth in British Overseas Territories* (Routledge, 2021). He is regularly invited to serve as a consultant to various inter-governmental and international organisations. Dominic is also a barrister, called to the Bar of England and Wales by the Honourable Society of the Inner Temple, and is a Door Tenant at Goldsmith Chambers, London.

Dr Dominic Thomas-James
LL.B. (Hons), M.Phil., Ph.D. (Cantab), Barrister (Inner Temple)

Editor, FraudNet Global Report

E. dominicthomasjames@cantab.net

Part V

Investigations, Ethics, Evidential Considerations and Other Selected Issues

Technology in Investigations and Evidentiary Considerations

Craig Heschuk, John Moscow & Alex Clarke

Abstract

As criminals and fraudsters have adopted emerging technologies to perpetrate crime, the investigation and enforcement community is responding by embracing technology that can even the playing field. In this article, Craig Heschuk, John Moscow and Alex Clarke discuss the use of technology and Artificial Intelligence in investigations and some of the issues which may arise when court orders directing disclosure are sought based on evidence arising from such investigations. The article concludes with advice for the effective drafting of a disclosure order or other court application based on digital investigations such as those provided by GreyList Trace Ltd.

1. Introduction

Asset tracing must be, by its very nature, a constant game of catch up as the bad guys seek every possible means, including cutting edge technology, to secret away their ill-gotten gains. Despite all of the formidable skills and experience brought to bear by investigative firms, law enforcement agencies, law firms and forensic accountants, recovery is far from certain for the victims of a fraud.

2. The Role of Artificial Intelligence in Combatting Fraud

The challenge for those of us in the industry is to adopt technologies that will "power up" investigations and thereby shift the struggle in favour of the good guys. In that regard the use of artificial intelligence ('AI') tools has the potential to be transformational. Using sophisticated algorithms, it is now possible in large and very complex investigations to achieve far better outcomes in terms of speed, cost and accuracy. As criminals get smarter and their networks for global funds transfer keep evolving, a technology-focussed response looks like an indispensible way forward. AI permits the global investigation of vast repositories of data to cut through much of the complexity and unpredictability associated with deciphering a sophisticated criminal network of special purpose corporations and bank accounts.

Being on the side of the angels comes with some challenges however. Legal and ethical standards necessitate a disciplined approach to compliance with applicable computer misuse and data privacy

laws. The asset recovery investigator is faced with the compelling necessity to ensure the results of an investigation can be used where it matters – in enforcing legal rights against criminals. At the end of the day, the work product of an investigation will often be scrutinized in a litigation process and in front of the courts. Having the technology to find relevant evidence is one thing – but ensuring the evidence is admissible requires some additional diligence which is necessary to win a proper result.

3. Technology Solutions – A Quick Review of The Existing Toolkit

Technological innovation has already generated a range of e-tools. Often these are specialized products and capabilities that are provided by third party service providers. In that context, let us start with a quick survey of a few of the key technologies available for fraud investigators. The following are some of the most powerful e-tools available.

3.1. E-Discovery and Digital Forensics

One of the most indispensable services for law firms, insolvency professionals and companies involved in disputes is e-discovery, digital forensics and AI-driven data analytics. Only the very largest firms can justify having in-house capability to analyze big data and so specialist service providers bring advanced computing power and dedicated expertise to sift through massive amounts of data and billions of data points. This permits the investigator to identify potential claims, isolate critical evidence in support of a claim and develop a narrative of the events that led to insolvency or to a bad actor committing a fraudulent act.

Alex Clarke of LDM Global describes the power of digital forensics as follows:

"Through the use of machine learning, natural language processing and entity extraction, systems can be trained to uncover patterns, detect emotions and sentiment behind communications, and isolate relevant information that supports a claim." He goes on to describe LDM's fraud investigation capability this way: "In situations where fraud is possible, LDM Global uses emotional intelligence to apply the fraud triangle framework within a database. The fraud triangle explains that the risk of fraud increases when an individual is under pressure, they've identified an opportunity to exploit, and when they've rationalised or justified their actions. With a few clicks, our AI systems can filter through millions of documents to isolate only those which exhibit high levels of pressure, opportunity and rationalisation."

3.2. GreyList - AI for Tracing Banking Relationships

The GreyList Trace platform allows investigators to establish whether an email address (of a person-of-interest) has been used to open and operate a bank account with any of the roughly 220,000 banks in the world. By combining algorithms with a sophisticated bank database, and without ever infiltrating a bank's computer systems, GreyList can identify, with a very high degree of accuracy, each of the banks where an individual has a banking relationship or has had one in the recent past. The means used are ingenious and rely on testing with software code that is innocuously "bounced off" the spam filters for all of the banks. No confidential information is obtained and no computer

systems are accessed in the testing. There is a more detailed discussion of GreyList below but, in simple terms, GreyList determines by deduction if the email address of the person-of-interest has been "whitelisted" by any of the banks. This results in a 98+% certainty as to the existence of banking relationship with the identified banks.

3.3. Cryptocurrency and Blockchain Analysis

The emergence of cryptocurrencies and their rapid adoption has led to the growth of a number of firms that specialize in cracking the blockchain for law enforcement and other clients that have justifiable cause to examine suspect crypto-transactions. Given the pervasive level of fraud and money laundering in electronic currencies, these services are indispensable for tracking criminal conduct – whether it is garden variety theft, sanctions evasion or terrorist financing.

Each of these technologies has potential application in large and complex fraud investigations. And in each case there are issues to be considered when gathering, analyzing and storing this information for purposes of potential future litigation.[1]

4. Admissibility Considerations

Generally speaking, evidence is admissible in legal proceedings if it is relevant to prove the facts of a case, but neither the evidence itself nor the means by which it was obtained may violate the law. There are particular considerations when the evidence is being obtained through technological means, and we will discuss the central issue of "provenance and authenticity" below. Importantly though, each technology tool has its own methodology and the issues around admissibility will be different for each.[2]

4.1 Provenance and Authenticity

The reliance on, and prevalence of, digital evidence that is submitted to the court in support of claims is growing in lockstep with the exponential growth of electronically stored information ('ESI') that is created, shared and stored during the course of day-to-day business functions. In consequence, the methods of preserving and maintaining the integrity of ESI in its original, unaltered state is becoming more complex and, in most cases, requires the assistance of forensically trained professionals who are experienced in handling digital evidence.

---

[1] Frowis, M et al., Safeguarding the evidential value of forensic cryptocurrency investigations, Forensic Science International: Digital Investigation, https://doi.org/10.1016/j.fsidi.2019.200902; Lawton, D et al., eDiscovery in digital forensic investigations, CAST publication number 32/14 available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/394779/ediscovery-digital-forensic-investigations-3214.pdf; United Nations Office on Drugs and Crime (UNODC) E4J Module, Digital evidence admissibility, available at https://www.unodc.org/e4j/en/cybercrime/module-4/key-issues/digital-evidence.html

[2] Lawton, D et al., eDiscovery in digital forensic investigations, CAST publication number 32/14, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/394779/ediscovery-digital-forensic-investigations-3214.pdf

Below, Alex Clarke discusses LDM Global's approach to the challenge of preserving the integrity of ESI:

"LDM Global's forensic experts are trained to maintain meticulous logs and unbroken chains of custody records to ensure that our collection and analysis methodologies and most importantly all evidence submitted to court, is admitted and withstands scrutiny from opposing parties. With any evidence, regardless of its form, its vital that the origin and authenticity can withstand scrutiny from opposing parties. However, digital evidence defined as, "… information stored or transmitted in binary form that may be relied on in court."[3], is unique compared to hard copy evidence in that the same evidence in its digital form consists of metadata and artifacts that are easily altered through the normal course of business or during forensic collections and analysis. Therefore, it's vital for any potentially relevant data to be preserved to prevent alteration and that defensible forensic collection methods are used to extract ESI."

4.2. Extraction of Data and the Challenge of Defensible Collection

E-discovery, digital forensics and blockchain investigations generally rely, to varying degrees, on the extraction of data from electronic sources. E-investigators have to carefully document their work and exhaustively prepare for potential challenges to the admissibility of evidence. Experts, in their respective disciplines, ensure that the evidence presented to the court is an identical hash duplicate (in layman terms, a hash value is a digital fingerprint that is used to authenticate digital evidence) of the original evidence and that all preservation, collection and analysis methodologies withstand the oppositions scrutiny.

4.3. Data Privacy Considerations

The techniques that are applied must be lawful of course which means that they must also be defensible in terms of data privacy requirements. In this respect, if information that can be construed as "personal data" is being processed then the means used must comply with the principles of relevant data privacy laws and there must be a "lawful basis" for processing the data.[4]

5. GreyList As A Case In Point

In the case of GreyList the level of intrusion is, in fact, minimal. Data extraction is essentially non-existent and the data privacy issues are likewise minimized. It is fascinating to realize that with this technology: (1) no data is extracted at all; and (2) no personal data is obtained. The system operates by deduction from the response of a spam filter.

Here's how GreyList works:

1. A client provides GreyList with one or more email addresses;
2. GreyList does not use the email address but instead creates a string of digital code;
3. The string of code, not the email address itself, is then loaded into the GreyList algorithm;

[3] National Institute of Justice (NIJ), Digital Evidence and Forensics, available at: nij.ojp.gov/digital-evidence-and-forensics

[4] UK Information Commissioner's Office (ICO), Guide to the General Data Protection Regulation (GDPR), available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

4. The code is sent out to interrogate the spam filters protecting every bank in the world;
5. The string of code does not contain any personal information nor any recognizable content; it has the "scent" of the email address being investigated, but that is all;
6. Spam filters are programmed to accept, reject, or further investigate incoming emails. Those email addresses that are recognised and authorised are on the bank's "whitelist." The time it takes the spam filter to process a whitelisted email versus a non-authorized email is significantly different, even though the timing difference is measured in milliseconds;
7. The GreyList Algorithm can detect this timing difference;
8. All of the software code tests are rejected at the spam filter level. Nothing enters the bank's computer servers. For this reason, the GreyList Algorithm does nothing more than indicate by deduction that a banking relationship exists. It cannot identify an account number, nor the account balance, because to do so would mean interacting with the bank's servers, which is precisely the level of intrusion GreyList is designed to avoid.

This is a tremendous benefit to the client and their legal counsel. The method of interrogation at the spam filter level is not only of negligible intrusion, but the required documentation for "provenance and authenticity" is simplified tremendously. Each investigation has the same technical process and is conducted on the same basis as all of the others. There is only a single interrogation process going on. Information is not being extracted from myriad discrete sources as in the case of a traditional big data digital forensics process.

6. Court Ordered Disclosure – Practical Considerations for Subpoenas and Other Court Orders Directing Disclosure

Court applications relying on technology-driven investigations have to take into account not only the evidentiary considerations around provenance and authenticity described above, but they also have to be carefully crafted to achieve the desired result.

Using GreyList's technology as an example, John Moscow of Lewis Baach Kaufmann Middlemiss offers the following analysis:

"In tracing assets it is frequently necessary to invoke the power of the Court to compel the production of evidence from a third party, or from the counter-party. In making an application to the Court you obviously need to know what you want and why you want it, but you need to be able to explain why you think that the party being compelled should be bothered at all.

In the past it would frequently happen that one would issue a subpoena in a civil case to multiple banks—or all of them (in the geographic area) if the case warranted that effort and expense. But, as alluded to above, bank accounts can be opened remotely, all over the world. That change gave a great edge to the fraudsters. The technological response to locating banks around the world is Greylist, which can identify each bank worldwide with which the email has been in touch. Once the banks are located the asset tracers need to go to the banks, consistent with local law, to obtain a subpoena, or a different court-order, directing the bank to produce what is asked for.

In drawing up the request, attention needs be paid to what you are seeking and why you think the party has it. After a Greylist connection is established, a subpoena to the bank should, at a minimum, ask for all email communications between the initial email and the bank's email. Although Greylist cannot provide the text of the emails, court process can compel its production and on receipt of the text of the communications the relationship of the bank and the target should be clear. How do you

get the subpoena? That depends on local law, but the key fact is the same: Greylist has established the fact of communication, so you are entitled to know what it was—and to follow up on that."

7. Conclusion

The use of artificial intelligence tools in investigations not only implies the use of cutting-edge technology but also the application of specialized methodologies to maintain the integrity of the information and ensure the investigation results can be used as evidence in court proceedings. It is important to use reputable investigation firms with transparent methodologies and established compliance programs in order to satisfy evidentiary requirements. Perhaps most importantly, retaining qualified legal counsel is critical to tailoring any court-ordered disclosure request to the particular requirements of the case and the evidence that is being relied on. Every case is different and a well-crafted subpoena (or other disclosure order application) can ensure your investment in pursuing a wrong-doer will yield dividends.

About the Authors

Craig Heschuk, Executive Vice President, Greylist is a legal and management professional with 30 years experience in commercial project development. He was admitted to the Canadian Bar Association in 1990. His career spans dozens of countries starting in the early 1990's when he was advising a major Canadian energy company on international projects. His subsequent experience includes 17 years living abroad with his family in Abu Dhabi, Singapore, Doha and Quito. His career has centered on corporate/commercial work, mainly in the development of major infrastructure projects in the energy, real estate and manufacturing sectors. Most notably he has acted as General Counsel to companies involved in upstream oil & gas development in South East Asia and utility-scale solar and wind power projects in Europe and elsewhere.

John Moscow, Senior Counsel, Lewis Baach Kaufmann Middlemiss PLLC**,** is well known and highly respected in the field of white-collar criminal law, where he has spearheaded and been involved in some of the most complicated fraud cases of the past 25 years. Driven by the complex facts of the matters facing his clients and possessing the ability to manage unprecedented legal issues, John has led investigations and conducted prosecutions and defenses involving money laundering and theft by high-ranking corporate individuals and major financial institutions both domestically and throughout the world. John spent 30 years with the New York County District Attorney's Office, where he prosecuted international economic crime, securities fraud and criminal violations of fiduciary duties. His knowledge and involvement in the investigation and prosecution of cases involving financial and corporate fraud led to the development of the theory of jurisdiction that has become widely adopted by lawyers prosecuting cases out of Manhattan. In private practice he has handled forfeiture cases for a foreign government, for third party claimants and for defendants

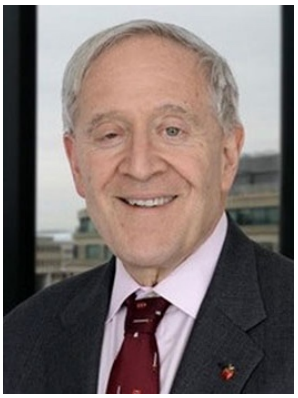
Alex Clarke is Director of LDM Global's Caribbean and Latin American territories, who is experienced with data handling and analysis, conducting forensic investigations, investigation fraud and assisting clients with sophisticated technology and eDiscovery solutions. He's assisted clients with addressing high-value multijurisdictional disputes including intellectual property, financial misstatements, embezzlement, fraud, employee termination and various other types of disputes.

Craig Heschuk
Executive Vice President

Greylist
E. craig.heschuk@greylisttrace.com

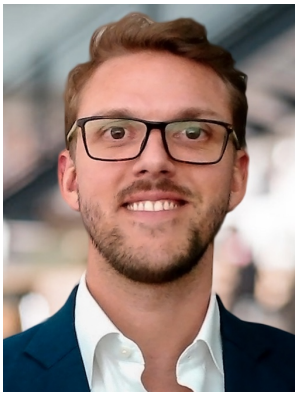
John Moscow
Senior Counsel

Lewis Baach Kaufmann Middlemiss PLLC
E. John.moscow@lbkmlaw.com



Alex Clarke
Director of Caribbean and Latin America

LDM Global
E: aclarke@ldmglobal.com



Greylist TRACE

The Impact of the Invalidation of the Privacy Shield on Global Investigations

Karen Schuler & Christopher Beveridge

Abstract

In this article, Karen Schuler, Governance, Risk & and Compliance Practice Leader and co-leader of BDO's Global Privacy Team, and Christopher Beveridge, Director and Head of Privacy and Data Protection, at BDO United Kingdom discuss the practical impact of the invalidation of the privacy shield on global investigations. Data continues to grow exponentially giving rise to vast amounts of invaluable evidence that could be subject to data transfer regulations, such as the European Union's General Data Protection Regulation ('GDPR'). Privacy regulations like the GDPR not only present operational changes, but they often present challenges for investigators that collect data in one country and need to transfer it to another country for analysis, review or evidentiary purposes. Given the invalidation of the EU-US Privacy Shield in July 2020, this article provides an overview of the history of the Privacy Shield Framework as well as considerations for global investigative teams when they are transferring data from the European Union to the United States.

Background and History of the EU-U.S. Privacy Shield

The goal of the EU-US Privacy Shield Framework was a framework that regulates transatlantic exchanges of personal data for commercial purposes between the European Union ('EU') and the United States ('US'). A primary purpose was to enable U.S. companies to more easily receive personal data from EU entities under EU laws, such as the GDPR, that are meant to protect the rights and freedoms of EU citizens. The EU-US Privacy Shield Framework replaced the International Safe Harbor Privacy Principles, which were invalidated in 2015. Following is a summary of activities that have occurred over the last several years as it relates to these privacy frameworks:

- In 2015, the fifteen-year-old U.S.-EU Safe Harbor framework was invalidated by the European Court of Justice ('ECJ').

- On July 12, 2016, the European Commission deeming the EU-US Privacy Shield Framework *"adequate to enable data transfers under EU law"*.
- Following the ECJ decision, the Swiss Government, on 12 January 2017, approved the Swiss-US Privacy Shield Framework as a *"valid legal mechanism to comply with Swiss requirements when transferring personal data from Switzerland to the United States"*
- [1].
- On 16 July 2020 the ECJ issued a judgement declaring the European Commission's Decision 2016/1250/EC of 12 July 2016, the EU-US Privacy Shield, invalid.
- Following the ECJ's decision in July, on 8 September 2020, the Federal Data Protection and Information Commissioner (FDPIC) of Switzerland invalidated the Swiss-US Privacy Shield framework.

Given the invalidation of the EU-US Privacy Shield Framework, the European Data Protection Board ('EDPB') has issued frequently asked questions on the invalidation of the Privacy Shield and has recommended that *"you must conduct a risk assessment as to whether Standard Contractual Clauses (SCC's) provide enough protection within the local legal framework, whether the transfer is the U.S. or somewhere else"*[2].

EU-US Privacy Shield Framework Controversy

Over the years there has been continued controversy as to the validity of the Safe Harbor and the Privacy Shield Frameworks. Most notably are the cases that were filed by Maximillian Schrems, an Austrian data privacy activist who initially sought to raise awareness around the misuse and lack of protection of personal data by Facebook by relying upon the Safe Harbor Framework to transfer data between the EU and the US. In this case, the Irish Data Protection Commissioner ('DPC') refused to investigate a complaint by Mr. Schrems where he requested that the DPC suspend data transfers from Facebook Ireland to Facebook Inc. due to concerns that the Snowden revelations suggested his personal data could be accessed by US intelligence agencies and that Mr. Schrems' EU data protection rights would be violated. This case (*Schrems I*) was referred to the Court of Justice of the European Union (CJEU) and in 2015 where they ruled that European Commission's adequacy determination for the US-EU Safe Harbor framework was invalid.

As a result of the invalidation of the Safe Harbor framework invalidation, Facebook began to rely upon another valid data transfer mechanism, Standard Contractual Clauses ('SCC's'). SCCs are standard sets of contractual terms and conditions by which the data exporter and the recipient of personal data agree to adequately protect personal leaving the European Economic Area ('EEA'). Under Article 46 of the GDPR, SCC's aim to provide appropriate safeguards for international data transfers provided that the SCC's are adopted completely and unaltered[3].

Data exporters and the recipient of the data that rely on SCC's to transfer personal data to a third country must, on a case-by-case basis, undertake necessary levels of due diligence to demonstrate that the recipient in the third country ensures adequate protections under EU law for any personal data transferred. If these safeguards cannot be achieved, the data exporter must then

[1] See: https://www.privacyshield.gov/program-overview.
[2] See: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/07/updated-ico-statement-on-the-judgment-of-the-european-court-of-justice-in-the-schrems-ii-case/.
[3] See: https://www.gtgadvocates.com/why-use-the-standard-contractual-clauses/.

consider using additional safeguards or they will be required to suspend the data transfer. Further to this it should also be noted that Supervisory Authorities now have the power to suspend transfers where they take the view that the party residing in the third country does not have an adequate level of protection in place required by EU law.

Following Facebook's use of SCC's, Mr. Schrems once again filed another complaint on the basis that the SCC's did not provide adequate security measures to individuals to protect the processing of their personal data, stating that US intelligence authorities would still be able to monitor this data. In November of 2019, this case was forwarded to the CJEU for review. Ultimately, on 16 July 2020 the EU-US Privacy Shield was invalidated (*Schrems II*) in its decision in *Facebook Ireland v. Schrems*[4]. However, the court ruled that SCC's are still a valid mechanism to transfer data from the EU to third countries.

The Impact of the Invalidation of the EU-U.S. Privacy Shield on Global Investigations

Global investigations rely on collecting data in a forensically sound and defensible manner, which can be challenging in and of itself. To add to the complexity of ensuring that data collections are handled in a defensible manner, privacy obligations must be considered and met to ensure that additional issues do not arise during the actual collections or the transfer of data to a third country. The invalidation of the EU-US Privacy Shield presents organizations with a new level of care before data is transferred from the EU to the US. If SCC's are invalidated in the future, then companies will need to rely on one or more of the following to legally transfer data during an investigation:

- *Article 49*[5] *– Derogations for Specific Situations*, which are exemptions from or relaxation of a rule or law and in *Schrems II* decision. The Court states that its decision to invalidate Privacy Shield won't create a "legal vacuum" for data transfers because organizations can still turn to Article 49 derogations. The EDPB references derogations as an available mechanism for continuing to transfer data to the US provided the conditions set forth in Article 49 apply[6]. From the viewpoint of an investigator, it is important to remember that available derogations include: (1) explicit consent, (2) required to perform a contract, or (3) there are compelling legitimate interests.

- *Article 47*[7] *– Binding Corporate Rules ('BCRs')*, which are data protection policies adhered to by companies established in the EU for transfers of personal data outside the EU within a group of undertakings or enterprises[8]. These rules require that all general data protection principles and enforceable rights are deployed to ensure that there are appropriate safeguards in place to protect the data transfer. It is important for investigators to recognize that there is a process for submitting BCR's for approval and that the process can be lengthy.

[4] See: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf.
[5] See: https://gdpr-info.eu/art-49-gdpr/.
[6] See: https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/07/20200724_edpb_faqoncjeuc31118.pdf.
[7] See: https://gdpr-info.eu/art-47-gdpr/.
[8] See: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en.

Continued guidance will continue to frame the way data collections are performed for years to come. As such, forensic investigators should familiarize themselves with regulatory guidance from the EEA, its member countries, and the US as it could impact future data collection practices and require certain obligations. Additionally, investigators should familiarize themselves with Article 46 and member country guidance. Article 46, the transfers subject to appropriate safeguards, provides detailed requirements that investigators should consider. For more information about this article, visit the United Kingdom's Information Commissioner's Office.

According to the Privacy Shield Framework's website[9], investigators should understand that:

- The US Department of Commerce and the European Commission and EDPB remain in close contact to 'limit negative consequences' of the decision to the transatlantic data flows.
- The US Secretary of Commerce and European Commissioner for Justice jointly stated in August 2020 that the two agencies are evaluating the potential for an enhance EU-US Privacy Shield Framework that will comply with the July 16th judgement in the *Schrems II* case.
- The Department of Commerce will continue to administer the Privacy Shield program while these discussions continue, including processing submissions.

While we await further guidance, investigators should continue to monitor media channels and authorities to gain an understanding of their obligations. It is extremely important during this time to consult with your general counsel, compliance office, or outside counsel to ensure that your team is taking appropriate steps to manage data transfers from the EU to the U.S. when conducting an investigation.

Recommendations

While we cannot foresee the outcome of the next version of the EU-US Privacy Shield investigators can adhere to standard practices to minimize risk. Steps to consider when conducting an investigation include, but are not limited to:

- Evaluate data transfer needs and the risk this imposes for your organization or your client. If you are an outsourced investigator consider reviewing your contracts with legal counsel to ensure that you are meeting the obligations as outlined in the invalidation of the EU-US Privacy Shield Framework. For in-house investigators, determine whether binding corporate rules have been approved.
- Determine whether you have derogation that allows for the transfer of data to the US from the EU.
- Ensure that your company (outsourced or in-house investigators) do not violate the GDPR, which could impose penalties of 4% of global turnovers or €20 million, whichever is greater.
- Continue to document and maintain sound record keeping practices to demonstrate that your organization is fully accountable for data transfer conclusions. It is no longer acceptable to sign

[9] See: https://www.privacyshield.gov/article?id=EU-U-S-Privacy-Shield-Program-Update.

the SCC's and file them away. The entire investigative team needs to understand the standard contractual clauses to ensure that they are followed.

- Consider whether Brexit will impact your data transfer mechanisms of personal data being transferred from the UK to other parts of the EU, and vice versa.
- Keep your eyes open for *Schrems III*; it's very possible there is another suit to follow.

Additional technical considerations that investigators should follow include:

- Processing must take place in a transparent manner, which may differ than that of the US. Custodians may need to be identified and notified that their data will be processed in conjunction with an investigation.
- Processing is limited to what is necessary to the investigation. This could result in more stringent searches and filtering to eliminate data that is perceived as unnecessary.
- The purpose for which the data can be used is limited. The investigator must limit the number of individuals that can access the data on the forensic servers and review platforms, as well as ensure that the data is only processed for its intended purposes.
- Appropriate administrative and technical safeguards must be implemented to ensure the data is protected at all stages of the investigation.
- Questions that the investigator should consider are: (1) what is the value of the data to the investigation? (Don't collect if you don't need it); (2) is the level of effort to collect the data synonymous with its value to the investigation?; or, (3) can the data be collected locally or are remote collections required? If the latter, ensure that data privacy regulations are not violated.

Appropriate administrative and technical safeguards that investigators can follow are generally outlined in Article 32[10] of the GDPR, which require:

- The employment of appropriate levels of security, and that data collection, processing and analysis risks are identified;
- Data encryption, especially when in transit;
- Current technical and organizational measures that are tested on a regular basis to ensure that policies and procedures align with current guidance, frameworks and best practices; and,
- That organizations adhere to an approval code of conduct as outlined in Article 40[11] or Article 42[12].

Companies conducting global investigations need to understand their obligations, their clients' obligations, as well as the role they play in safely transferring data from the EU to the US. Even though initial guidance was provided by the US Department of Commerce and the European Commissioner for Justice, investigators should continue to monitor official information related to the EU-US Privacy Shield.

[10] See: https://gdpr-info.eu/art-32-gdpr/.
[11] See: https://gdpr-info.eu/art-40-gdpr/.
[12] See: https://gdpr-info.eu/art-42-gdpr/

About the Authors

Karen Schuler has a broad background in managing businesses that provide governance, risk management and compliance (GRC) services. With nearly 30 years of experience she has built and managed organizations that provide data protection, digital forensics, cyber investigations, and e-discovery, and data breach notifications, as well as having focused those teams and her career on providing subject matter expertise across the GRC spectrum. Karen currently serves as the Data Protection Officer (DPO) for Fortune 50 and Fortune 1000 companies across several industries. In her capacity she has worked with Data Protection Authorities, Supervisory Authorities and Data Subjects on EU Global Data Protection Regulation (GDPR) obligations. As well she regularly reviews and evaluates privacy operations, individual rights management capabilities, and data governance requirements. And, finally, she works with her privacy clients to ensure global compliance and to assist them with establishing privacy and governance operations.

Christopher Beveridge is a Director within Risk Advisory Services and is Head of Privacy & Data Protection for BDO LLP.
As a qualified chartered accountant, Christopher delivers audit, advisory and business consultancy services to clients within the United Kingdom and around the world. Specialising in advising and assisting clients on data protection and privacy issues which includes the UK Data Protection Act and the EU General Data Protection Regulation (GDPR). This involves educating organisations on the subject, writing and advising on privacy policies and procedures and the general management of these activities across any organisation. Chris now also acts as a DPO for a number of organisations through the outsourced DPO service offering that BDO provides. Chris is also a member of the International Association of Privacy Professionals ('IAPP') and holds the Certified Information Privacy Professional - Europe (CIPP/E) qualification.

Karen Schuler, CFE, CIPP/US, CIPM, FIP, CDPSE
Principal and Governance, Risk & Compliance Practice Leader
BDO USA

E. kschuler@bdo.com

Christopher Beveridge
Director, Head of Privacy and Data Protection
BDO LLP

E. Christopher.Beveridge@bdo.co.uk

Ethics in Without Notice Orders – Frankly, the Judge Needs to be Told

Lance Ashworth QC & Matthew Morrison

Abstract

In this paper, Lance Ashworth QC and Matthew Morrison of Serle Court Chambers look at the duty to give full and frank disclosure when seeking orders without notice to the opposing party. The applicable principles in England and Wales are considered along with an analysis of the High Court's current position as to how stringently this duty must be complied with. This is contrasted briefly with the apparently more lenient position in the British Virgin Islands ('BVI'). Of particular interest is the requirement, as part of the duty to give full and frank disclosure, to make relevant inquiries before seeking such an order.

1. Introduction

As barristers, we will often be instructed in a fraud case where there has been no interaction with the other side, and where therefore we will only hear one side of story. Normally, we will have a highly motivated client who feels strongly that they have been wronged and that there is (and can be) no innocent explanation. Every experienced practitioner knows that the law is full of open and shut cases that turn out to be no such thing: even when nothing concerning turns up in the documents, and the view that the case is unlosable persists all the way up to one's client entering the witness box, it can all go horribly wrong at that point.

In relation to freezing orders, there have recently been a number of cases both in England and Wales and further afield where the requirements of the duty of full and frank disclosure, and the consequences of failing to comply with that duty, have been stringently applied with serious adverse consequences for the claimant. There is a feeling that, in particular, the Commercial Court in London is becoming more wary of granting freezing orders, one of the two nuclear weapons in the lawyer's armoury.

So, unless the risk of dissipation of assets is extremely imminent, it is essential that time is taken to get things right and to avoid adding to the injustice the client will have suffered of having been

defrauded by being ordered to pay substantial costs to the alleged fraudster before the proceedings have got very far.

2. Full and frank disclosure – the principles

The starting point of any adversarial system of justice is that the Court should hear from both sides before making any decision. There is a high risk of error if the Court does not allow the affected party to be heard. As well as the harm that can be caused to a respondent, hearing only one party risks undermining the integrity of the Court's process. In *Fundo Soberano De Angola v Jose Folimeno Dos Santos*[1] Popplewell J went so far as to hold that compliance with the duty of full and frank disclosure is necessary to enable the Court to fulfil its own obligations to ensure fair process under Article 6 of the European Convention of Human Rights.

It is clear that if a without notice application is made, the Judge needs to be able to trust the lawyer(s) appearing before the Court to tell the Judge everything that he/she needs to know. This is achieved by giving full and frank disclosure and not by instructing a barrister well versed in the area and whom the Judge may "trust". It is notable that some of the decisions below have been in cases where recognised leaders in their field have been representing the ultimately hapless claimants.

3. What is full and frank disclosure?

The modern statement of requirements is usually taken to be the judgment of Ralph Gibson LJ in *Brink's Mat Ltd v Elcombe*[2]. These include:

- Materiality is to be decided by the Court not by the applicant or its advisers;
- Proper inquiries must be made before making the application: it is not only material facts that are known which need to be disclosed, but any additional facts which would have been known if had made such inquiries;
- The extent of the inquiries depends on the circumstances of the case: that is the nature of the case; the effect of the order; the degree of urgency and the time allowed for inquiries;
- If a breach of the duty is found, the court will be astute to ensure that no advantage is secured;
- Whether the breach is sufficiently material to require immediate discharge of the order depends on the importance of fact to judge: whether the breach was innocent or otherwise is important but not determinative;
- In the event of a material non-disclosure, the Court has discretion to continue the order or to re-make the order on new terms.

Subsequent case law has made clear that the duty to give full and frank disclosure:

- Includes matters of law and procedure as well as of fact[3];

[1] [2018] EWHC 2199 (Comm) at [51]
[2] [1988] 1 WLR 1350 at 1356 as long ago as 12 June 1987: a couple of years before the Berlin wall came down, the same year Mrs Thatcher secured her third term and one of the authors was called to the Bar.
[3] *Memory Corp Plc v Sidhu (No.2)* [2000] 1 WLR 1443 at 1460.

- Continues to apply at all times until Respondent can themselves discharge it[4], so that matters arising between obtaining the order and service must be brought to the attention of the Court[5];
- Means that the lawyers must fairly present matters which are disclosed[6] and specifically identify the points for and against the order being sought rather than relying on general statements and the mere exhibiting of numerous documents[7];
- Requires the Court to be told if evidence (no matter how compelling) has been obtained by improper or illegal means such as covert recordings or hacked emails[8];
- Applies to clients as much as lawyers[9].

These principles are not applicable only to freezing orders but apply to any without notice application. They extend, for example, to applications for permission to serve proceedings out of the jurisdiction, which is a relief frequently sought at the same time as obtaining a freezing order[10]. Given how important and familiar these principles are, it might be thought surprising that applicants still fall foul of them.

4. When will the Court discharge the without notice Order?

Along with pressures lawyers can feel when told by a client that there is a clear and obvious fraud with the perpetrator about to abscond with the ill-gotten gains, in the authors' experience the degree of rigour to which the principles have been applied, and sanctions have been imposed, has ebbed and flowed over time.

There was for a long time concern about unmeritorious applications to discharge for the most trifling of non-disclosures. In *Brink's Mat* itself, Slade LJ sounded a note of caution, observing that a number of respondents appeared to be leaning on the principle as representing substantially the only hope of obtaining the discharge of injunctions where there was little prospect of doing so on the substantial merits of the case or the balance of convenience.

This concern has not dissipated, so that sixteen years later when faced with an application in *Kazakhstan Kagazy Plc v Zhunus*[11] to discharge in which 82 paragraphs of an affidavit set out extensive

---

[4] Although if at any stage subsequent to the order being imposed, even after the order has been confirmed on the return date, it comes to the attention of the claimant that there had been a failure of full and frank disclosure, the claimant should bring that to the attention of the Court and seek to have the order confirmed, as happened in *SITA UK Group Holdings Ltd. v. Serruys* (unreported 18/2/2010). This was the conclusion reached by Eder J in *Speedier Logistics v. Aardvark Digital* [2012] EWHC 2776 at [25].
[5] *Commercial Bank of the Near East v A, B, C and D* [1989] 2 Lloyd's Rep 319.
[6] *The Arena Corp Ltd v Schreer* [2003] EWHC 1089 (Ch) at [117].
[7] *The Siporex Trade SA v Comdel Commodities Ltd* [1986] 2 Lloyd's Rep 428 at 437.
[8] *St Merryn Meat Ltd v Hawkins* [2001] C.P. Rep. 116; *Dar Al Arkan Real Estate Development Company v. Al Refai* [2012] EWHC 3539 (Comm).
[9] *Fundo Soberano* (supra) at [53].
[10] In *Evison Holdings Ltd v. International Company Finvision Holdings LLC* [2020] EWHC 239 (Comm) it was held that the duty extended to telling a Commercial Court the test for service out of the jurisdiction when the Judge would deal with the application on paper.
[11] [2014] EWCA Civ 381 at [35]-[37].

allegations of non-disclosure, Longmore LJ considered it necessary to repeat guidance first given in the unreported decision of Toulson J in *Crown Resources AG v Vingradsky*[12]*:*

- Issues of non-disclosure ought to be capable of being dealt with concisely;
- It is inappropriate to seek to set aside a freezing order for non-disclosure where proof depends on establishing facts which are themselves in issue in the action, unless they are truly so plain that they can be readily and summarily established;
- The court must maintain a sense of proportion and have regard to relevance and the overriding objective;
- The more complex the case, the more fertile the ground for alleging non-disclosure: accordingly the more important it is that the Judge should not lose sight of the wood for the trees.

However, it is possible to detect a thawing in the Court's reluctance to discharge for failure to comply with the duty of full and frank disclosure. In the *Fundo Soberano* case, Popplewell J said that if there is a material breach of the duty, then even if there is a good basis for the order, the order is likely to be set aside on the return date, and no fresh order made.

A similarly robust approach has been taken in the British Virgin Islands at first instance by Jack J in two cases arising in the *Abyzov/Vekselberg* or *Renova v Emmerson* litigation in May and July 2019 respectively. Jack J discharged two orders made on New Year's Eve 2018 holding that there had been non-innocent breaches of the full and frank disclosure obligations (combined in the earlier decision with a finding that there had been a complete lack of remorse or contrition for the breach). That said, the Court of Appeal in the Eastern Caribbean Supreme Court ('ECSC') subsequently took a more lenient view in *Paraskevaides v. Citco Trust Corporation Ltd*[13] on an appeal from the High Court of the BVI. The ECSC appeared to adopt the position that the court will not reimpose relief if the failure to make full and frank disclosure was not innocent, but holding on the facts of that case (and overturning the first instance Judge's finding that such failure had not been innocent) that the failure arose from an innocent failure to perceive the relevance of a key letter on certain issues and accordingly, the without notice order should not be discharged.

Need to investigate

Two recent decisions of the High Court in England appear to have set the bar high in terms of the extent to which parties are required to conduct an investigation into relevant adverse matters. The first of these is *Rogachev v Goryainov*[14]. This was a dispute arising out of a joint venture to operate farmers' markets in Moscow. While this might be thought to be a quaint operation, it was in fact a large scale venture involving the injection of approximately US$50 million of capital. The joint venturers decided to part ways. Proceedings were brought in England, in which it was alleged that the respondent had sought to dispose of one of the sites unilaterally and clandestinely: the sale was specifically said to have been concealed from the claimant and only discovered by chance. One of the grounds upon which it was held that there had been a breach of the full and frank disclosure

[12] Unreported (15th June 2001).
[13] BVIHCMAP2018/0046 (CA 30 March 2020).
[14] [2019] EWHC 1529 (QB).

duty was that there was an advert for the site on a Russian property website many months before the claimant said he had become aware of the property sale. The Judge found that the claimant had not known of this:

"*[h]owever, that fact was discoverable by more careful inquiry on the part of the Claimant*"[15].

Had it been discovered, the claimant could not have told judge that the respondent was acting clandestinely. The order was discharged.

The second is the decision of Carr J in *Tugushev v. Orlov*[16]. The Judge cited thirteen relevant principles which were said to be non-contentious and well established, including that:

"*An applicant must make proper enquiries before making the application. He must investigate the cause of action asserted and the facts relied upon before identifying and addressing any likely defences. The duty to disclose extends to matters of which the applicant would have been aware had reasonable enquiries been made. The urgency of a particular case may make it necessary for evidence to be in a less tidy or complete form than is desirable.* ***But no amount of urgency or practical difficulty can justify a failure to identify the relevant cause of action and principal facts to be relied on.***"[17] (emphasis added).

The claim was based upon an alleged conspiracy by the respondent and two associates by which the claimant said he had been unlawfully deprived of a 1/3rd share in a large international fishing business. Among the material non-disclosure found by the Judge was a failure by the claimant to disclose that he had divested himself of his shareholding and made declarations to that effect in 2003 upon taking public office. Carr J was sceptical about his claims to have forgotten these events but was willing to proceed at an interlocutory stage on the basis that this was an unintentional oversight. Mr Tugushev invited her Ladyship to conclude that his duty of reasonable inquiry did not extend to matters in 2003 and 2004 which he did not recall. Carr J rejected this in stringent terms:

"*His failure to investigate whether or not he had signed such declarations was a reckless disregard of his duty of full and frank disclosure to the court, particularly in light of Mr Orlov's express contentions of which Mr Tugushev was well aware. Those contentions required Mr Tugushev to consider very carefully whether they might be correct and make relevant enquiries*"[18].

Carr J was also clear that even if Mr Tugushev had forgotten about this, he could not reasonably have been sufficiently certain to make categorical statements in his evidence to the effect that he never signed any such documents. At a minimum the claimant should have made inquiries of the relevant authorities, and had he done so, the documents would have come to light.
While Carr J reiterated the need to avoid a scattergun approach on such an application, and the imperative of avoiding a mini-trial about disputed points that would be resolved in underlying proceedings, she nevertheless emphasised that:

---

[15] Supra at [89].
[16] [2019] EWHC 2031 (Comm).
[17] Supra at [7(iv)].
[18] Supra at [30].

"*immediate discharge (without renewal) is likely to be the court's starting point, at least when the failure is substantial or deliberate*"[19].

This is so even if the order would still have been made had the relevant matter been brought to its attention at the without notice hearing.

Carr J made no bones about fact that "*this is a penal approach and intentionally so, by way of deterrent to ensure that applicants in future abide by their duties*"[20]. It follows from her decision that a Court is unlikely to regrant an order, even if there was not deliberate non-disclosure, where there has been a failure properly to investigate before making the without notice application.

Conclusion

The following conclusions can be drawn from the principles and cases referred to above:

- Neither the lawyers nor the client can decide not to make inquiries because they fear that something unhelpful might be discovered.
- Given the draconian effects of a freezing order, seeking to excuse the making of inquiries on the grounds of urgency is unlikely to carry much weight unless there is a very strong case of urgency, and is not going to wash when the application has been put together over a number of weeks.
- Experience shows that what the client and lawyers think is not material may be very material in the eyes of the Judge. Therefore, it is quite possible that the lawyers may have considered some information, genuinely decided it is not material and therefore not disclosed it, only to find that the Judge thinks it is highly material and consequently discharges the injunction on the return date. The lesson has to be to err to an extreme extent on the side of caution and disclose much more rather than less.
- If evidence has been obtained improperly or unlawfully, this must be disclosed. The evidence will still be admissible and while the Judge may not approve of what has been done, a failure to tell the Judge is inevitably going to lead to the order being discharged when the truth comes out.
- If there has been a deliberate failure to give full and frank disclosure, there is in reality no prospect of maintaining an order obtained without notice, no matter how strong the case against the fraudulent defendants is.
- Whether a Court will decline to discharge the order, or discharge but impose a fresh order may well be influenced by the question of whether the non-disclosure was innocent or otherwise, but this is by no means determinative and, at least in England, there seems to be a move against regranting orders obtained even where the failure was innocent.
- It is likely the innocent claimant will be visited by a swingeing costs order, payable immediately to the fraudulent defendant.

It is therefore extremely important to take time to investigate properly before launching such an application. This is a matter which is required of lawyers as part of their duty to the Court and

[19] Supra at [7(x)].
[20] Supra at [7(xi)].

therefore a matter of ethics. If there is a deliberate non-disclosure by lawyers (a conclusion that every lawyer dreads a Judge reaching on the return date of a without notice order), the consequences faced by the lawyers will go further than mere ethics.

About the Authors

Lance Ashworth QC *MA (Cantab), Barrister (Middle Temple)* is a barrister practicing out of Serle Court Chambers, London. He was called to the Bar of England and Wales in 1987 and became a Recorder in 2005. He took Silk in 2006 and was appointed a Deputy High Court Judge in 2016. **Matthew Morrison** *MA (Oxon), BCL, Barrister (Lincoln's Inn)* is a barrister practising out of Serle Court Chambers, London. He was called to the Bar of England and Wales in 2004 and was admitted to practice in the Cayman Islands in 2005. Lance and Matthew practise in the fields of civil fraud, commercial litigation, company and partnership, and insolvency, among other areas. They have done a number of cases together, including *Instant Access Properties v. Rosser* [2018] EWHC 756 (Ch) in which they successfully defended a fraudulent trading claim for approximately £35 million, arising out of the off plan sales of properties in Florida and *Re Galasys*, an allegedly fraudulent attempt to have an AIM company delisted. Both have a strong international dimension to their practices. Lance has recently been involved in cases involving allegations of fraud and/or bribery said to have happened in Ethiopia, the United States of America, Canada, France, Spain, Ireland, Portugal, Malaysia and Bahrain. Matthew has been enjoying the ease of international travel in the Zoom era which has facilitated his attendance at hearings in the Courts of the British Virgin Islands, Dubai International Financial Centre, Jersey and Guernsey from the comfort of his own home.

Lance Ashworth QC

Serle Court
E. lashworh@serlecourt.co.uk
T. 02072426105

Matthew Morrison

Serle Court
E. mmorrison@serlecourt.co.uk
T. 02072426105

serle court

The Financial Conduct Authority and a Sample of its Enforcement Activity

Professor Stuart Bazley

Introduction

Throughout much of 2020, the UK's financial services industry has been dealing with the impact of the Covid-19 pandemic. This has included the UK Financial Conduct Authority ('FCA' or 'Authority') giving necessary attention to the supervision of authorised firms' resilience during the pandemic and the impact that the economic conditions may have on market volatility[1]. Notwithstanding such necessary emphasis, the FCA has continued to engage in enforcement activity.

This article examines some of the FCA's important criminal prosecutions and associated civil enforcement activity since December 2019. These relate to the FCA's work in guarding the very perimeter of the regime for persons carrying on regulated financial services activity, the law prohibiting abuse of the financial markets and criminal law provisions of the Financial Services and Markets Act designed to support some of the FCA's powers of investigation.

The perimeter

The question of whether financial services activity in the UK requires authorisation and regulation is far from simple. Part II of the Financial Services and Markets Act 2000 (FSMA) along with the Financial Services and Markets Act Regulated Activities Order[2] set out those activities which, when carried on by way of business, require authorisation (or exemption), whether by the UK Prudential Regulation Authority or FCA. Indeed it is an offence under s23 of FSMA to carry on regulated activity by way of business without authorisation or exemption. Authorisation is critical for the effective operation of some of what many regarded as safety-net provisions under FSMA. For

[1] FCA Business plan 2020/21. The Financial Conduct Authority 7 April 2020 https://www.fca.org.uk/publication/business-plans/business-plan-2020-21.pdf accessed 13 December 2020.
[2] Financial Services and Markets Act 2000 (Regulated Activities Order) 2001/544 (as amended).

instance, the Financial Services Compensation Scheme only has jurisdiction to provide compensation to consumers where an authorised person is unable to meet liabilities to customers.[3]

In its perimeter report for the period 2019 and 2020, published on 29 September 2020, the FCA provides some indication as to the complexity of the regulatory regime and the difficulty that it creates for determining which side of the perimeter activity falls.[4] For instance, in that report the Authority states:

'The UK financial services industry is broad, carrying out a wide range of activities for UK and international clients. Some of this activity requires FCA regulation and some of it does not. We call the distinction between what is regulated, and what is not, the 'perimeter.'[5]

The Authority also recognises that during the current Covid-19 economic climate an increase in criminal activity may include unauthorised financial activity, stating in its perimeter report: *' These are challenging times. We are aware that the coronavirus (Covid-19) crisis may exacerbate specific perimeter issues and encourage unlawful activity, impacting vulnerable consumers and SMEs especially.'*[6]

Nonetheless the FCA is active in its work to safeguard the perimeter of the regulated financial services market and secure compensation for any victims of such activity, although not all action it takes relies on the criminal law. Arguably because of the Authority's limited resources, it may not take formal enforcement action (whether criminal or civil) in every case of unauthorised activity.[7] In its 2020 perimeter report the FCA gives an indication of the types of circumstances where it is more likely to act, stating:

'…we are more likely to act where the unregulated activity:
- *is illegal or fraudulent*
- *has the potential to undermine confidence in the UK financial system*
- *is closely linked to, or may affect, a regulated activity…'*[8]

The end of 2019 saw the FCA publish the outcomes of confiscation orders obtained in relation to two previously successful criminal convictions for unauthorised investment activity. On the 20 December 2019 the Authority announced it had obtained an order for the confiscation of £171,913.60 of realisable assets against Mr Manraj Singh Virdee following his guilty plea to charges in relation to the operation of an unauthorised investment scheme, as the sole director of a business known as Dynamic UK Trades Ltd.[9] The monies confiscated were to compensate victims who has

[3] See s213 Financial Services and Markets Act 2000.
[4] The Financial Conduct Authority Perimeter report 2020/21, 29 September 2020. <https://www.fca.org.uk/publication/annual-reports/perimeter-report-2019-20.pdf> accessed 13 December 2020.
[5] n4 para 1.2.
[6] n4 pg3.
[7] For comment on the FCA resource and the number of firms it regulated see the opening paragraph of the Chair and Chief Executive message FCA Business plan 2020/21 page 3 at n1.
[8] n4 para 2.5.
[9] FCA Press release *'FCA secures confiscation order totaling over £170,000 against convicted fraudster'* The Financial Conduct Authority 20 December 2019 < https://www.fca.org.uk/news/press-releases/fca-secures-confiscation-order-totalling-over-170000-against-convicted-fraudster> accessed 12 December 2020.

lost money following his unlawful activity. The FCA reported that during the confiscation order proceedings, the court found that Mr Virdee had benefited from £666,730.58 from his activities with most of it being lost through his unsuccessful trading or being used personally. [10]

Earlier, on 17 December 2019, the FCA announced that it had obtained a Confiscation Order totalling £5,118,018.72 against Mr Dharam Prakash Gopee along with an order for him to pay over £200,000 in compensation.[11] Mr Gopee had operated illegal lending between 2012 and 2016 (a period of time during which the regulation of consumer credit activity was transferred to the FCA) resulting in his conviction in 2018 for illegal money lending contrary to s39(1) Consumer Credit Act 1974 and s23(1) Financial Services and Markets Act 2000.[12] The FCA had outlined in a 2018 press release following Mr Gopee's sentencing that the offences included him engaging in new lending of around £1 million and the taking of payments for both new and existing loans of around £2 million.[13] In addition to the confiscation order, due to the circumstances of the case and Mr Gopee's activities, the FCA had also obtained a Serious Crime Prevention Order as a way of stopping him carrying out in future his unlawful activity.[14] In addition Mr Gopee had also been convicted for contempt as a result of not complying with the terms of a restraining order. [15]

Market abuse

On 24 September 2020 the Authority announced that it had commenced criminal proceedings against three individuals formerly employed by a company named Redcentric plc.[16] On 26 June 2020 Rednectric had been the subject of a public censure from the FCA in connection with market abuse (details of which are set out further below.) The FCA set out in its 24 September press release that the three former employees appeared before Westminster Magistrates court on 23 September 2020, with Mr Fraser Fisher (Redcentric's former Chief Executive) charged with two counts of making a false or misleading statement contrary to s89 (1) the Financial Services Act 2012; Mr Timothy Coleman its former Chief Financial Officer charged with two counts of making false or misleading statement contrary to s89(1) Financial Services Act 2012, four counts of false accounting contrary to S17(1) (a) of the Theft Act 1968, one count of making a false or misleading statement to an auditor contrary to s501 Companies Act 2006, and one count of fraud by false representation contrary to sections 1 and 2 Fraud Act 2006; and Ms Estelle Croft, the company's former finance director, being charged with two counts of making a false or misleading statement contrary to s89

[10] n9.
[11] FCA Press release 'FCA secures confiscation order totaling £5million against illegal money lender' The Financial Conduct Authority 17 December 2019. < https://www.fca.org.uk/news/press-releases/fca-secures-confiscation-order-totalling-5-million-against-illegal-money-lender> Accessed 12 december 2020.
[12] FCA Press release 'Dharam Prakash Gopee guilty of acting as an illegal money lender' the Financial Conduct Authority 8 February 2018. https://www.fca.org.uk/news/press-releases/dharam-prakash-gopee-guilty-acting-illegal-money-lender Accessed 12 December 2020. For the background to the case see R v Gopee [2019] EWCA Crim 601.
[13] FCA Press release. 'Convicted illegal money lender sentenced to three and a half years imprisonment' The Financial Conduct Authority 9 February 2018 < https://www.fca.org.uk/news/press-releases/gopee-convicted-illegal-money-lender-sentenced> Accessed 12 December 2020.
[14] n13.
[15] n13 and R v Gopee [2019] EWCA Crim 601.
[16] FCA press release *'FCA Institutes criminal proceedings against three former employees of Redcentric plc'* The Financial Conduct Authority . 24 September 2020 < https://www.fca.org.uk/news/press-releases/fca-institutes-criminal-proceedings-against-three-former-employees-redcentric-plc> accessed 12 December 2020.

(1) the Financial Services Act 2012, seven counts of making of making a false or misleading statement to an auditor contrary to s501 Companies Act 2006, and four counts of false accounting contrary to s 17(1) (a) Theft Act 1968.[17]

Redcentric plc had been subject to an FCA civil law regulatory enforcement decision (i.e. not a criminal law case) in respect of market abuse contrary to s118(7) Financial Services and Markets Act 2000, namely the dissemination of false or misleading information.[18] That provision was in force at the time relevant to Redcentric's conduct, but has since been replaced by Article 12 of the EU Market Abuse Regulation now setting out a range of market manipulation behaviours.[19]

S118(7) FSMA provided,

'…the behaviour consists of the dissemination of information by any means which gives, or is likely to give, a false or misleading impression as to a qualifying investment by a person who knew or could reasonably be expected to have known
that the information was false or misleading."[20]

Redcentric plc is a public company with its shares admitted for trading on the London Stock Exchange's Alternative Investment Market. The background to the FCA's decision, as set out in its Final Notice, concerned a misstatement in the company's published interim results for its half year to 30 September 2015 in which it set out that its net bank debt position was £16.5 million and it had cash and cash equivalents of £9,984,000, and year end results to 31 March 2016 where it stated total net borrowings of £25.3 million and cash and cash equivalents of £8,492,000.[21]

In relation to the Final Notice to Redcentric, the FCA's Director of Enforcement and Market Oversight, Mr Mark Steward, stated:

'Publicly listed companies must ensure the market is properly informed with timely and true information. In this case, Redcentric issued misleading final year results, harming its own investors and confidence in the market. When the company revealed the true position in November 2016, many investors who had purchased Redcentric shares in the preceding 12 months suffered immediate losses. These losses are directly attributable to the misleading statements issued by the company 12 months earlier. Investors deserve to be told the truth and uncomfortable news cannot be hidden for very long.'[22]

Of particular note is the FCA's decision to publicly censure Redcentric and not impose a civil law financial penalty. Part of the basis of this aspect of the FCA's decision appears to be because of the

---

[17] n16.
[18] FCA Final Notice to Redcentric plc 26 June 2020 The Financial Conduct Authority https://www.fca.org.uk/publication/final-notices/redcentric-plc-2020.pdf accessed 12 December 2020.
[19] Regulation (EU) No 596/2014 on market abuse (market abuse regulation).
[20] See s118 (7) Financial Services and Markets Act 2000 replaced 3 July 2016 See Financial Services and Markets Act 2000 (Market Abuse) Regulations 2016/680.
[21] n18.
[22] FCA press release 'FCA publicly censures Redcentric plc for market abuse' The Financial Conduct Authority, 26 June 2020 https://www.fca.org.uk/news/press-releases/fca-publicly-censures-redcentric-plc-market-abuse accessed 12 December 2020.

company's proactive response. This included a 'forensic' review of both its current and historic balance sheet positions, and a remedial plan established by the company to compensate shareholders disadvantaged as a result of the market abuse, which resulted in a payment of £11.4 million.[23]

In relation to the remedial action taken by Redcentric, Mr Steward stated:

'In this case Redcentric has agreed to provide compensation for affected investors to make good the losses while also preserving the company's ongoing business at a time when the business is providing vitally needed services in the fight against coronavirus (Covid-19). We welcome the Redcentric board's decision as well as the steps taken to remediate the company's governance.'[24]

More recently, on the 16 December 2020, convictions for insider dealing by Fabiana Abdel-Malek (a compliance officer at an investment bank) and Walid Choicair (a day trader) were upheld by the Court of Appeal.[25] The original prosecution followed an FCA investigation and the resulting conviction was concerned with Mr Chocair trading on price sensitive information that he had received from Ms Abdel-Malik who was an insider. The appeal however, was concerned with whether the convictions were unsafe because of allegations of the FCA's insufficient disclosure. Commenting on the Court of Appeal's dismissal of the case, Mark Steward, the FCA's Executive Director of enforcement and market oversight said, *'I welcome the Court's decision to dismiss these appeals as well as the Court's finding that there was no irregularity or unfairness in the proceedings. The appeal was an attempt to undermine the jury's verdict by collaterally attacking the FCA. Today's decision by the Court vindicates the FCA's decision-making in this matter.'* [26]

The criminal law and the FCA's powers of investigation

FSMA provides the FCA with a range of formal powers of investigation – many of which may be relied on by the FCA during regulatory/civil law investigations. Additionally, however, s177 FSMA provides for criminal offences that may be committed in connection with an FCA investigation.

The trial at Southwark Crown Court of the FCA's first prosecution of the offence of destroying documents contrary to S177(3) (a) Financial Services Act 2000, however resulted in a not guilty verdict for the defendant Mr Konstantine Vishnyak.

It is an offence under s177(3) (a) FSMA where *'…a person who knows or suspects that an investigation is being or is likely to be conducted under Part XI of FSMA is guilty of an offence if he falsifies, conceals, destroys or*

[23] See for instance, RNS Redcentric *'Accounting misstatements'* 7 November 2016 <https://ir.q4europe.com/solutions/Redcentric/3172/newsArticle.aspx?storyid=13476302 > accessed on 13 December 2020; RNS Redcentric 'Update on forensic review and remedial action plan' https://ir.q4europe.com/solutions/Redcentric/3172/newsArticle.aspx?storyid=13498018 accessed on 13 December 2020; RNS Redcentric 'Proposed restitution scheme…' 26 June 2020 https://ir.q4europe.com/solutions/Redcentric/3172/newsArticle.aspx?storyid=14737226>; and FCA Final Notice n 18 page 9.

[24] n22.

[25] R (the Financial Conduct Authority) v Fabiana Abdel-Malek and Walid Chocair [2020] EWCA Crim 1730.

[26] FCA press release, *'Insider dealing convictions upheld by the Court of Appeal'* The Financial Conduct Authority 16 December 2020. < https://www.fca.org.uk/news/press-releases/insider-dealing-convictions-upheld-court-appeal> accessed 23 December 2020.

otherwise disposes of a document which he knows or suspects is or would be relevant to such an investigation, unless he shows that he had no intention of concealing facts disclosed by the documents from the investigator…'

The prosecution was brought in connection with an FCA investigation into a suspicion of insider dealing , during which the FCA had requested Mr Vishnyak to provide the WhatsApp application on his mobile phone, and which the FCA alleged he deleted.[27]

The FCA's comment on the not guilty verdict was limited to a short press release statement that: *'The FCA is disappointed with the outcome, but respects the verdict. We will take action whenever evidence we need is tampered with or destroyed.'*[28]

The cases outlined in this article touch on a number of fundamental areas of the FCA's enforcement work. As we look forward to 2021, although it is reasonable to expect the FCA's enforcement work in such areas will continue, one might consider the extent to which future FCA criminal and civil enforcement work will address activity associated with the impact of the Covid-19 pandemic on the financial markets. This has perhaps been already predicted by the FCA, which in its 2020 business plan states:

'*We will remain vigilant to potential misconduct. There may be some who see these times as an opportunity for poor behaviour – including market abuse, capitalising on investors' concerns or reneging on commitments to consumers.*

Where we find poor practice, we will clamp down with all relevant force…' [29]

About the Author

Stuart Bazley is a Visiting Professor at BPP University Law School, London where he teaches on its LL.M programme. Stuart has worked in the financial services industry since 1980, including holding senior appointments as an in house lawyer and compliance officer. He now works in the compliance function of a leading UK financial institution. Stuart is the author of *Market Abuse Enforcement: Practice and Procedure* (2013, Bloomsbury) and a co-author of *Market Abuse and Insider Dealing* (2016, Bloomsbury) now in its 3rd edition.

Professor Stuart Bazley
e. StuartBazley@BPP.com

[27] FCA press release *'Konstantin Vishnyak appears at court for destruction of documents offence'* The Financial Conduct Authority 6 September 2019< https://www.fca.org.uk/news/press-releases/konstantin-vishnyak-appears-court-destruction-documents-offence> accessed 23 December 2020.
[28] FCA press release. *'Konstantin Vishnyak found not guilty of destroying documents'* the financial conduct authority, 28 september 2020. Https://www.fca.org.uk/news/press-releases/konstantin-vishnyak-found-not-guilty-destroying-documents accessed 12 December 2020.
[29] n1 page10.

Collateral Attacks on Funders as a Defense Tactic in Asset Recovery and Fraud Claims

James C. Little & Christopher N. Camponovo

In 1998, during the notoriously corrupt and brutal regime of General Sani Abacha, Nigeria's then-Minister of Petroleum, Chief Dan Etete, awarded the rights to exploit an oil field known as OPL 245 to a company named Malabu Oil and Gas Ltd ('Malabu'), of which he secretly was part owner.[265] Over a decade of machinations, in-fighting, and litigation, the controversy was "resolved" through the government (including some of the same officials who were part of the original award) agreeing to a deal in which Malabu and Etete withdrew their claims and OPL 245 was awarded to a consortium led by Italian oil giant, Eni, in exchange for a payment of $1.3 billion. Of that $1.3 billion, only $200 million went to the Federal Republic of Nigeria ('FRN'). The rest – $1.092 billion – went to Malabu and Dan Etete, who in turn, paid off a number of Nigerian public officials, including then President Goodluck Johnathan.

Two years later, after reports of the payments to FRN officials became public, the Public Prosecutor of Milan, Italy ('PPM') commenced a criminal investigation into allegations that senior executives of Eni and Royal Dutch Shell had knowledge of, and indeed encouraged, the corrupt payments, and had received or agreed to receive payments in the form of reverse commission or kickbacks. In December 2017, the Milan court accepted the recommendation of the PPM and ordered Eni, its executives (including the current and former CEOs), and their co-defendants to stand trial for the crime of international corruption.

The year before the Milan trial began, the FRN appointed a Nigerian law firm, Johnson & Johnson, as its agent to recover assets misappropriated through the various OPL 245 transactions. Given the magnitude and breadth of litigation that would be necessary, Johnson & Johnson concluded an agreement with a litigation funder, Drumcliffe Partners LLC, to finance its efforts. To date, Johnson & Johnson has recovered nearly $83m for the FRN, and is pursuing legal action in

[265] This is a story best told without the distraction of legal citation and, accordingly, we dispense with the formality. For those wishing to check the details and confirm the accuracy of the matters discussed herein, the facts are compellingly laid out in the work of NGOs (https://www.globalwitness.org/en/campaigns/oil-gas-and-mining/opl-245-shell-and-enis-nigeria-deal/), the opinions of both the English Commercial Court and the Federal District Court for the Southern District of New York, as well as the myriad pleadings and submissions of the parties – in Delaware, Milan, London, Lagos, and Quebec.

eight jurisdictions to recover the proceeds of the fraud. Notably, the FRN has appeared in the criminal trial in Milan as a *parte civile* in order to assert its right to civil damages resulting from the crimes committed.

As the Milan trial entered its final phase and the defendants began presenting closing arguments, Eni filed an *ex parte* motion under 28 USC sec. 1782 in Delaware, seeking permission to serve intrusive discovery on Drumcliffe – notably, documents and deposition testimony regarding (1) the identities of Drumcliffe's beneficial owners/or ultimate stakeholders; (2) Respondents' relationship to current or former FRN officials; and (3) any contractual and/or financial arrangements that Drumcliffe has entered into with respect to the OPL 245 proceedings. Eni's discovery application, and the legal theories it claims that discovery will support, are premised on a tenuous and discredited conspiracy theory that Eni sources entirely to internet media reports. According to Eni, Drumcliffe stands to earn a windfall from the litigation brought by the FRN's recovery agent, and has therefore managed to induce the FRN (possibly through backdoor deals with unnamed Nigerian officials) to bring unsubstantiated claims against Eni and to stonewall Eni's ongoing efforts to exploit OPL 245. Eni claims that it intends to use evidence of this alleged conspiracy in the Milan proceedings, and in an ICSID arbitration which Eni filed only days before the 1782 motion.

Eni's application exemplifies a growing trend in asset recovery finance, and in litigation funding in general, where deep-pocketed defendants accused of civil and criminal wrong-doing engage in collateral attacks against funders in order frustrate the claims against them.

The strategy rests on three fundamentally flawed assumptions. First, defense counsel assume that expenditure of additional capital will cause the funder to stop funding the claim. Second, they believe they can drive a wedge between the funders and plaintiffs by causing a funder to focus on self-preservation at the expense of the core claim. Third, they hope that by making the terms of funding agreements public, judges will be less willing to award damages to a plaintiff because part of the proceeds will go to the funder.

But these assumptions are misguided. First, in any high-value commercial dispute, the costs of defending third-party discovery efforts generally pale in comparison to the funder's overall financial commitment to the core claim. Second, in our experience, these discovery attacks only galvanize the relationship between the funder and its client (Drumcliffe and Johnson & Johnson) – simply by laying bare the continued malfeasance of the wrongdoer (Eni). Finally, as a result of the growth of the litigation financing industry, judges are rarely surprised to learn litigation is financed. As a fellow funder put it, all litigation is financed: by the plaintiff who pays his lawyers by the hour, by the lawyers who work on a contingency fee agreement, or by a third-party who pays the lawyers in exchange for a percentage of proceeds.

In the OPL 245 litigation, U.S. District Judge Maryellen Noreika issued an Order granting Eni's motion, which (as is common) was made on an *ex parte* basis, without hearing or opposition. Drumcliffe subsequently challenged the Order through a Motion to Vacate, Quash or Modify and/or for Protective Order. In its Motion, Drumcliffe framed Eni's discovery request as a meritless

attempt to exact retribution against a commercial litigation funder that has assisted the FRN — Eni's victim — in holding Eni responsible for its crimes. Drumcliffe argued that the relevant statutory and discretionary factors weigh heavily against the discovery, and also that Eni violated its duty of candor to the court by conjuring suspicion and intrigue where none exists, and by failing to disclose important facts, including that the evidentiary phase of the Milan trial has closed, and that the court is now hearing closing arguments. With its Motion, Drumcliffe submitted evidence in the form of an affidavit from its principal that:

- Drumcliffe has no direct relationship with the FRN, contractual or otherwise;
- All of its investors are domiciled in the United States, and none is a current or former FRN official;
- Drumcliffe is entitled to a percentage of J&J's small share of any recovery, not the FRN's share; and
- Drumcliffe does not have any rights to the direction, control settlement or conduct of the litigation.

Ultimately, Drumcliffe's position is that the information would be of no use to Eni, regardless of what cockamamie theory it presents to support its use in either Milan or with ICSID.

In its opposition to Drumcliffe's Motion to Quash, Eni recycles many of the arguments in its original 1782 Motion while at the same time creating a veneer of complications attendant to questions of Italian law – hoping the court will default to the path of least resistance and allow its Order to stand. It also claims Drumcliffe's description of its relationships with J&J and the FRN is too "carefully crafted," and therefore supports Eni's speculation a dirty deal is afoot.

As at the time of writing, Drumcliffe has not filed its Reply, and no hearing has been set. It is, therefore, entirely possible that even if Eni ultimately prevails, it will be too late to submit evidence in the Milan trial which is scheduled to wrap up in February 2021. This will leave Eni with limited options for deploying any discovery it obtains – on appeal in Italy (if it can overcome the high bar to admitting new evidence) or in the arbitration (where discovery traditionally is more limited than in the federal courts, and for which Eni has resisted enunciating a theory of relevance). Of course, none of this will matter to Eni if, as Drumcliffe has suggested, its primary goal in seeking this discovery is retributive.

What Eni's discovery application makes clear is that bad actors – if their pockets are deep enough – will use any and all means to avoid accountability, including the same legal tools that more commonly are deployed against perpetrators of fraud and corruption, instead of their victims. Ultimately, it is a fool's errand, but one which their high-paid defense attorneys are more than happy to run on a full-fee, hourly basis.

About the Authors

James C. Little is the Founder and CEO of Drumcliffe, the world's only litigation finance fund dedicated exclusively to asset recovery. Jim has overseen alternative investment portfolios involving aspects of asset recovery since pioneering the sector in 2008. Prior to founding Drumcliffe, he was a Managing Director at a London-based private equity fund with interests in real estate, capital markets, and venture capital. Jim has also held senior positions in the defense and national security industries.

Christopher N. Camponovo has over 20 years of experience as a public international lawyer, both in government and the private sector. He has held senior positions at the White House and U.S. State Department and has spoken, written and published on a diverse range of topics, including U.S. foreign investment treaties, international human rights, and corporate ethics.

James C. Little
(MPA, Harvard University; MA, Johns Hopkins University; BA, Marymount University)

Founder and CEO
Drumcliffe Partners

E. info@drumcliffepartners.com

Christopher N. Camponovo
(JD, University of California, Los Angeles Law School; BA, UC-San Diego)

Senior Counsel
Halcyon Law Group

E. info@drumcliffepartners.com

DRUMCLIFFE
A WORLD LEADER IN ASSET RECOVERY FINANCE

ICC FraudNet Strategic Partners

ICC Commercial Crime Services

Cinnabar Wharf
26 Wapping High Street
London
E1W 1NG
United Kingdom

Phone: +44 (0) 20 7423 6960
Fax: +44 (0) 20 7423 6961
Email: fraudnet@icc-css.org
Web: www.icc-css.org/home/fraudnet

FraudNet was founded in 2004 and operates under the auspices of ICC Commercial Crime Services – the anti-crime arm of the International Chambers of Commerce (ICC), the Paris based world business organization with offices in more than 90 countries.