



2022

ICC FraudNet Global Annual Report

Edited by
Dr Dominic Thomas-James

ICC FraudNet
COMMERCIAL CRIME SERVICES
est. 2004

2022

ICC FraudNet Global Annual Report

**The Ever-Evolving
Nature of Fraud and
Financial Crime:
International Insights
and Solutions**

Edited by
Dr Dominic Thomas-James



ICC FraudNet Global Annual Report 2022

Published by ICC FraudNet in 2022 on www.iccfraudnet.org

© 2022 ICC FraudNet, ICC Commercial Crime Services, Cinnabar Wharf, 26 Wapping High Street, London, E1W 1NH, United Kingdom

All rights reserved. No part of this publication may be reproduced, distributed, or otherwise transmitted in any form or by any means without the prior written permission of ICC FraudNet, except in the case of brief quotations embodied in promotional materials or critical reviews. Permissions can be sought, in writing, from above address.

The ICC FraudNet Global Annual Report 2022 is made up of individually-authored articles. The views expressed in these articles do not represent the views of ICC FraudNet, ICC Commercial Crime Services, the International Chamber of Commerce, or the Editor, and are the individual author's own views.



About ICC FraudNet

ICC FraudNet is an international network of independent lawyers who are the leading civil asset recovery specialists in each country. Using sophisticated investigation and forensic tools and cutting-edge civil procedures, FraudNet members have recovered billions of dollars for victims of some of the world's largest and most sophisticated global frauds involving insurance, commodities, banking, grand corruption and bankruptcy/insolvency. FraudNet was founded in 2004 and operates under the auspices of the Commercial Crime Services of the International Chambers of Commerce (ICC) – a Paris-based world business organization with offices in 90 countries.

ICC Commercial Crime Services
ICC FraudNet
Cinnabar Wharf
26 Wapping High Street
London
E1W 1NG
United Kingdom
Phone: +44 (0)20 7423 6960
Fax: +44 (0)20 7423 6961
fraudnet@icc-ccs.org
www.iccfraudnet.org
www.icc-ccs.org

Acknowledgments

The Editor wishes to acknowledge the following people who have been of instrumental value in the publication of the second ICC FraudNet Global Report. Mr Peter Lowe, Executive Secretary of FraudNet, has provided steadfast support and ongoing enthusiasm for this initiative. Mr Michele Caratsch and Mr Babajide Ogundipe have contributed significant guidance during this edition of the Report, as well as writing its foreword. The Editorial Board have been of great help throughout and consist of Mr Shaun Reardon-John, Mr Rodrigo Callejas, Mr Waseem Azzam, Mr Christopher Redmond, Mr John Greenfield and Mr Bruce Horowitz. The Editor wishes to thank all the authors of the 2022 Report for their intellectual engagement in this project and for contributing their thought-leadership to the ongoing debates in our field through this publication. The Report comprises contributions not only from FraudNet Members, but also from all of FraudNet's Strategic Partners. The Editor also wishes to thank the authors' staff who have been of great support throughout the editing and review stages. Thanks also to Ms Priya Jethwa, FraudNet's Director of Marketing and Communications, for her promotional efforts. Finally, gratitude to all FraudNet staff for their ongoing assistance in making this publication possible.



Executive Directors' Foreword

Michele Caratsch and Babajide Ogundipe

February 2022

We are pleased to commend this, second, FraudNet Global Report. We hope will be as well received as the first. During 2021, we all continued to struggle with the effects of SARS-CoV-2. Nevertheless, many of our Members and all our Strategic Partners managed to convene in Barcelona, Spain in November 2021 for an in-person meeting, when it appeared that the world was, slowly, inching towards putting the worst of the disease behind it. Omicron arrived and suggested that such hopes may have been a little premature. The most recent scientific opinion indicates that 2022 may indeed see a significant improvement in how we live our lives with this disease. It is with this hope that we have approached 2022.

At our Barcelona meeting, we were able to discuss some of the developments contained in the first Report, and we are hopeful that some of the material contained in this second Report will form part of our discussions at our next meeting, which we hope to hold, again in-person, during May of this year. This report, following on from the first, once again features articles on developments related to our practice area contributed by our Members and Strategic Partners, as well as leading academics engaged in research relating to economic crime, risk, financial regulation and compliance.

Our thanks go to the contributors and to our Editor Dr Dominic Thomas-James who has pulled everything together on schedule (as usual) and to the other members of the Editorial Board for committing their valuable time to this. How Dominic manages to do so much in such a timely fashion, given his other commitments, continues to be a source of wonder to us! We also thank our Executive Secretary, Peter Lowe, for his continued dedication to the network.

We hope readers will find this Report to be of value and we again invite you to share it widely and engage the contributors directly, or even by way of communications to the Editor. Such engagement might even become a feature the Editor may incorporate in future Reports.



Michele Caratsch



Babajide Ogundipe



Editor's Summary

Dr Dominic Thomas-James

February 2022

The second edition of the ICC FraudNet Global Annual Report takes as its theme the ever-evolving nature of fraud and financial crime, its responses and solutions. Ravaged and restricted by the Covid-19 pandemic – even at the point of publication – the current global climate of uncertainty has generated cause for re-thinking the responses to financial crime as its methods evolve. The annual Global Report published by FraudNet comprises original thought-leadership from its members and Strategic Partners. It represents a unique contribution to these increasingly global issues. Focusing on the network's interrelated practice areas of fraud, financial crime investigations and asset recovery, the papers herein exhibit expert insight from cutting-edge developments in the members' respective jurisdictions as well as important contemporary cases in which many members have been actively involved.

Building on the success of the first edition published in 2021, this 2022 Report comprises **28 original articles** authored by **46 contributors**, from some **22 jurisdictions** across the network. Many of the group have been involved in some of the most high-profile and complex asset-recovery cases, and their experience in this regard makes for fascinating, instructive reading. Articles come from contributors practising in the UK, USA, Ireland, Jersey,

Guernsey, Malta, Luxembourg, Poland, Spain, Austria, Hungary, Lebanon, Argentina, Guatemala, Panama, the Cayman Islands, the British Virgin Islands, Senegal, South Africa, Malaysia, Singapore and Japan; as well as from academics engaged in fraud and financial crime research. This breadth of engagement demonstrates the network's global reach.

In furtherance of FraudNet's thought-leadership and academic initiatives that I am privileged to lead, this journal highlights purposive and practically-relevant insights from leading practitioners, which it is hoped shall be of significant use to the wider network, Strategic Partners, professional collaborators, existing and prospective clients, and those with a practical, academic or policy interest in these important issues.

Mindful that we are still living in a pandemic, fraud and related financial misconducts have spiraled during Covid-19. Whether a confidence trick perpetrated by fraudsters manipulating the pandemic floodgates to unlawfully claim state benefit; or those targeting the vulnerable to exploit a sense of fear by pressuring them to part with savings for sham investments; or sophisticated, cross-jurisdictional cyber-frauds or

ransomware attacks on over-burdened public sector organisations – this environment of volatility and overstretched systems is fertile ground for fraud to thrive.

The Report is thematically divided into chapters for ease of reference, although it must be noted that many of the contributions herein overlap into other areas by nature of this inter-related subject. Some of the specific themes covered in the Report include criminal and civil asset recovery initiatives, insolvency-related misconduct, investigations – including forensic analysis, litigation financing and partnerships, cyber-fraud including the increase in technology threats, virtual assets and cryptocurrencies, transparency initiatives and beneficial ownership, forgery and counterfeiting, and offshore issues.

Just as the ease with which predicate criminality can be committed and facilitated in a transnational sense, so too is the ability to utilise a borderless global economy to hide the proceeds of crime and suspect wealth. The offshore world has, for example, since the last report come under increased scrutiny in the wake of the Pandora papers data-leak, and has faced fresh criticism as to the facilitative role that certain in their number may – knowingly or inadvertently – be playing. The leaks also shone an indefatigable light on ‘onshore’ centres. Further, since the 2021 Report, we have seen increasing fallout from the 2020 FinCEN files publication. While such data-leaks are becoming commonplace and seemingly supported by legislators committed to corporate transparency – if the public register provisions of the UK Sanctions and Anti-Money Laundering Act are anything to go by – the revelations contained in such publications are oftentimes relatively unsurprising to those in this field. However, their influence on policy and the ongoing debate is inescapable. The issue of beneficial ownership is, of course, not an issue

confined to the offshore world – but rather, as we saw with the US Corporate Transparency Act of 2021, there is increasing momentum in this area across the world, with the Financial Action Task Force engaging in an international consultation on a renewed standard. These issues are considered in the Report from both offshore and onshore perspectives.

Some of the contributions herein outline the utility of ‘controlled transparency’ in terms of global investigations of cases that involve some corporate presence offshore, as well as the benefits of litigating offshore or seeking injunctive relief therein to be enforced elsewhere. Members from the Cayman Islands, British Virgin Islands and Channel Islands share their practical insights on recent developments in this regard. In doing so, they also contribute deeper context to the often misunderstood world of ‘offshore’.

Elsewhere in the Report, the fundamental issue of the interplay between criminal and civil regimes is discussed – particularly in relation to operational synergy and cooperation between both frameworks as a means of enhancing investigations and their results.

Virtual currency is another key theme that is considered in the Report. It is increasingly controversial given the disparity by which both governments and regulators view certain virtual assets, and the challenges in a legal sense as to whether or not such “property” can be considered fair game in asset-recovery. This is set against a backdrop of concerns about how fraud can be perpetrated in the context of virtual assets. As the Head of the UK Financial Conduct Authority recently observed at the 38th Cambridge Symposium on Economic Crime, “many social media influencers are routinely paid by scammers to help them pump and

dump new tokens on the back of pure speculations". The application of new techniques in the virtual asset space is considered in the Report, including overviews of developments in jurisdictions like Malaysia, Singapore and Poland.

Important procedural issues are amply discussed, including enforcement of foreign judgments and the application of disclosure orders in terms of strategy. The continued application of relief such as Norwich Pharmacal orders are discussed, for example by reference to the Irish courts, as well as enforceability of judgments in certain jurisdictions, such as Lebanon.

The Report also considers forgery and counterfeiting in English law, as well as the position of professional advisors dealing with such cases. Further, one contribution reveals and analyses the industrial scale of wine fraud and forging in Europe.

The Report outlines developments in investigations, and insolvency-related misconduct. Insights are also provided from litigation funders highlighting challenges with spurious tactics used against funders during proceedings. Cutting edge accounts are provided in regards of the use of innovative technology to assist discovery and court proceedings. The theme of suspicious wealth is also considered in the Report including reviews of recent legal developments such as the impact of unexplained wealth orders in certain jurisdictions – a civil tool to target illicit wealth.

The network really demonstrates in this Report not only the breadth of work that members are engaged in, but also provides valuable observations from particularly high-profile cases. Insights from a contentious and ultra-high-net-worth case are given, in particular in relation to complex asset structures for high-value assets, and challenging, yet

fruitful, efforts to obtain restrictive orders across a variety of jurisdictions.

The Report comes at a time where FraudNet was able to host its first in-person meeting since Beirut in 2019. It was particularly pleasing to launch various thought-leadership initiatives during the pandemic, but even more rewarding that many of the insights and ideas contained in the first Global Report were able to be discussed in person in Barcelona in late 2021. We look forward to such future opportunity in, hopefully, a safer and less restricted world by the time the Spring meeting comes.

In order to advance integrity in our societies, disrupt economic crime, repatriate ill-gotten gains, and achieve meaningful legislative and regulatory developments in furtherance of this mission, it has never been more important for those at the coal face to contribute to the debate. It is only with a greater understanding of mutual challenges that shared responses can develop, and meaningful cooperation can take place. This is critical when so many cases are transnational in their scope and impact. FraudNet Members and Strategic Partners' engagement with this Report and the useful insights provided herein, contribute to this important objective and provide a basis for deeper understanding these complex issues.

Sincere appreciation to all contributing authors and colleagues in this field for making this Report possible. I hope the reader finds the 2022 Report instructive and insightful.



Dr Dominic Thomas-James

Contents

| | |
|--|-----------|
| About ICC FraudNet | 4 |
| Acknowledgments | 5 |
| Executive Directors' Foreword Michele Caratsch and Babjide Ogundipe | 6 |
| Editor's Summary Dr Dominic Thomas-James | 7 |
| The 33rd FraudNet International Conference: Barcelona | 14 |
| | |
| PART ONE: Criminal and Civil Developments in Fraud and Asset Recovery | |
| | |
| The Interaction of Criminal and Civil Process in Fraud Cases Stephen Baker | 17 |
| | |
| Evaluating different Unexplained Wealth Orders and Explaining their Effectiveness Diane Bugeja and Peter Mizzi | 27 |
| | |
| Recent Developments in Pursuing Claims Against Organized Crime Group Representatives in Japan Hiroyuki Kanae and Hidetaka Miyake | 38 |
| | |
| Who is the Victim and Who is the Fraudster? Reviewing the Procedural Position of the Victim in Fake President Fraud Cases, and How to Reframe it? Gábor Damjanovic and Réka Bali | 43 |
| | |
| Beneficial Ownership: An Overview of the Senegalese legal and institutional framework Dr Aboubacar Fall | 49 |



PART TWO: Enforceability

The Extraterritorial Application of Asset Forfeiture Proceedings in South Africa 60

Michael-James Currie, John Oxenham and Jemma Muller

Akhmedova v Akhmedov – a Case Study in Successfully Dealing with Difficult Defendants 69

Anthony Riem and Andrew McLeod

Ransomware Relief: A Review of the Development and Use of Norwich Pharmacal Orders in Ireland 82

Joanelle O’Cleirigh

Enforcement of Foreign Judgments in Lebanon 90

Nada Abdelsater

Hunting for Hidden Treasures in Austria with New Enforcement Rules – What to expect from the “Overall Reform” of Austrian Enforcement law? 97

Bettina Knoetzl and Katrin Hanschitz

PART THREE: The Offshore Dimension

No Stone Unturned: Tools of the trade available to the asset recovery lawyer in Guernsey 106

John Greenfield, David Jones, Robin Gist

Notes from a Small Island 118

Colette Wilkins QC, Nick Dunne and Andrew Gibson

Offshore – Decline or Thrive? Can the British Virgin Islands survive in a world of international minimum level tax treaties and data hacks and leaks? 125

Shaun Reardon-John

Beneficial Ownership Registers Offshore: An Update 133

Dr Dominic Thomas-James



PART FOUR: Cybercrime

Legal Developments in Malaysia on Cyber Fraud and Cryptoassets 141

Lee Shih and Nathalie Ker

Cybercrimes in Poland - Latest News 146

Joanna Bogdańska

PART FIVE: Virtual Assets

Applying Traditional Asset Recovery Techniques in the New World of Virtual Assets and Cryptocurrency 150

James A. Pomeroy

To Regulate or Not to Regulate: Law Enforcement, Criminal Cartels 160

and the Legitimation of Cryptocurrency

Kate McMahon

Coming to Terms with Crypto 173

Christopher Weil, Sean Anderson and Craig Heschuk

Cryptocurrency Disputes - Jurisdictional Challenges and Novel Solutions 178

Danny Ong and Stanley Tan

PART SIX: Insolvency-related Issues

Using Receiverships to Investigate and Combat Fraud 185

Joe Wielebinski and Matthias Kleinsasser

Recognition of Foreign Insolvencies in Panama 194

Donald Andersson Sáez Samaniego



PART SEVEN: Forgery

Wine Fraud in Spain: Has Over-Regulation of the Industry Led to Self-Sabotage? 200

Héctor Sbert

The Honest Forger and the Importance of Crying Foul: Insights on Forgery in English Law 206

Hugh Norbury QC and Dan McCourt Fritz

PART EIGHT: Investigations, Litigation Funding & Other Developments

Data Science for Investigations: A Practical Guide to Increasing Readiness 213

Jared Crafton

Resisting Challenges to Funding in Claims Against Fraudsters 220

Christopher N. Camponovo and Kirt W. Gallatin

Searching for the Debtors' Bank Accounts across the European Union: the EAPO Regulation Information Mechanism 230

Carlos Santaló Goris

The Financial Conduct Authority and NatWest Bank 243

Professor Stuart Bazley

FraudNet Strategic Partners 250

The 33rd FraudNet International Conference

Dr Dominic Thomas-James

International
Fraud and Asset
Recovery: Cases
and Strategies

Barcelona 2021

Between 4th and 6th November 2021, ICC FraudNet's Members and Strategic Partners BDO, Grant Thornton, Greylis Trace, Mintz Group and Drumcliffe, hosted the 33rd FraudNet International Conference in Barcelona at the Hotel Arts.

As this was the first 'in person' meeting since the outbreak of Coronavirus, it is fair to say that the network was eager to resume FraudNet's buoyant fellowship and collegial discussions that the pandemic had inhibited – at least in the physical sense. Of course, and unsurprisingly, our field of fraud and asset recovery did not observe the same degree of distancing that practitioners were observing.

Undeterred by restrictions and the ravages surrounding it, FraudNet's work continued and expanded throughout the pandemic, and the group had convened various remote meetings and conferences as well as launching other thought-leadership initiatives during this unprecedented time. But, given that the Barcelona meeting was the first of its kind since Beirut in late 2019, this was a keenly-anticipated reunion of members and colleagues.

Indeed, the sentiment during the meeting was very much one of enjoyment in seeing

colleagues and renewing close, professional relationships – including those new FraudNet members yet to attend an in-person event, and a keenness to deliberate and exchange insights. Despite the continuance of some international restrictions, the meeting was the largest to date in terms of scale, with over 125 participants over the course of the conference.

The meeting was entitled “**International Fraud and Asset Recovery: Cases and Strategies**”. Of course, the group had much to cover in this limited time – given the unprecedented challenges thrown up by Covid-19 in terms of fraud, as well as new techniques and tools which have developed since the last meeting. The programme comprised panel discussions, presentations by individuals and firms, break-out sessions, and some well-awaited opportunities to continue deliberations in a convivial environment – made all the more pleasant by the hospitality and culinary excellence of the Catalan region that we were fortunate enough to experience. The conference was also live-streamed for members and colleagues unable to travel to Spain.

Among the high-level contributions and insights throughout the conference by both speakers and participants, a flavour of those included insights around the niche area of wine forgery in Europe; the use of new technologies in identifying targets in asset recovery; a review of insolvency legislation; case study observations from a high-value divorce case and multi-jurisdictional recovery initiatives; the role of, and challenges faced by, litigation funders; the management of complex forensic investigations; transparency and cooperation at EU level; and the future of 'offshore'. We also had participation from leading academics sharing insights from their research in this field.

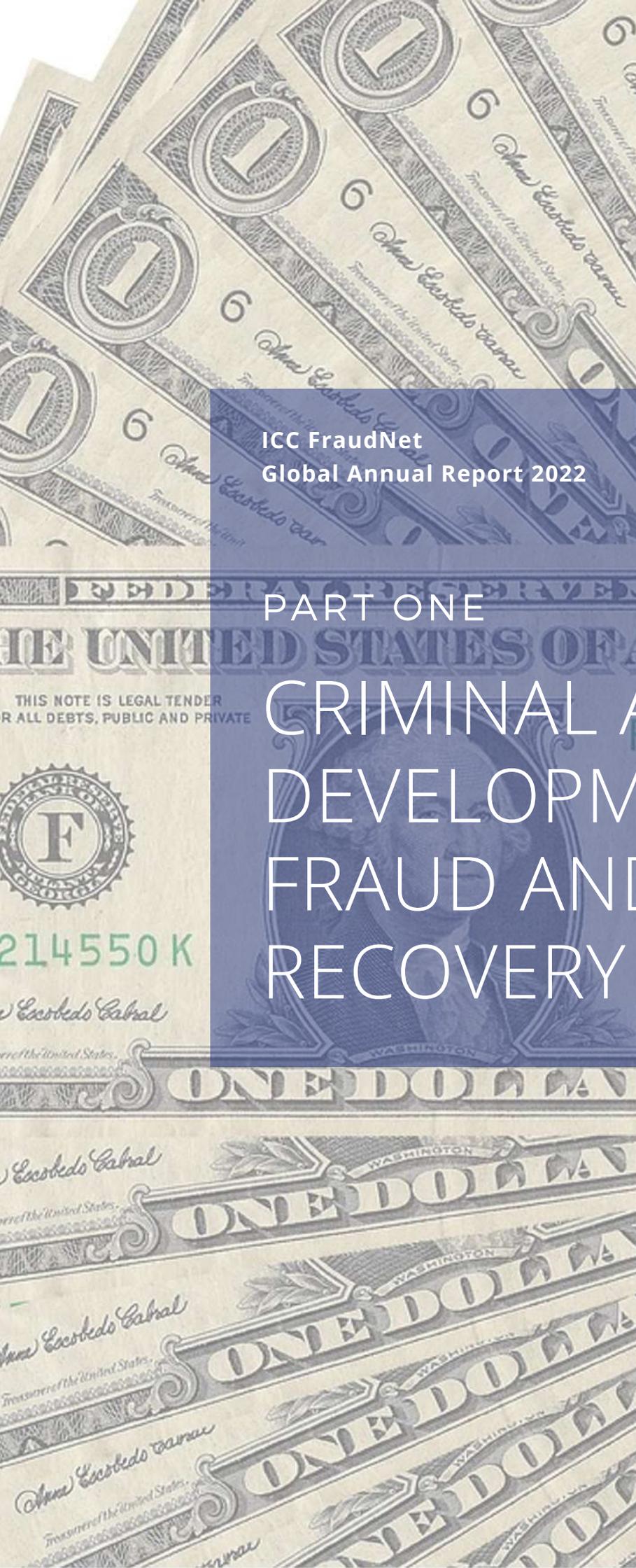
The conference was also a chance to promote a new initiative, 'FraudNet Future', and meet a new generation of FraudNet members and associates. Recognising the importance of continuity in the context of an elite network that has grown to such global strength since its 2004 establishment, this proved a useful means of introducing new members to the group - of which there were 18 in attendance.

Following the main conference, the group

attended a gala dinner at the Hotel Miramar where delegates continued discussions over cocktails in an orange grove overlooking Barcelona, followed by an exquisite dinner, speeches and prize giving. It was a chance to reflect on a tumultuous two years, the success of the Barcelona meeting, and the valuable professional connections nurtured within FraudNet.

Thanks to the organisers -too many to name - but particularly Mr Peter Lowe, Mr Michele Caratsh and Mr Babajide Ogundipe for their direction in making this meeting possible. Finally, to FraudNet's Spanish representative, Mr Héctor Sbert Pérez who, along with his colleagues Ms Maria de Mulder Rougvie and Mr Jaume Papasseit Fusalba, went to great local efforts to organise a comprehensive programme of events which was greatly received by the participants. Thanks to all members, Strategic Partners, their colleagues and guests who participated in Barcelona, and those who joined remotely, for their attendance and contribution to the success of this meeting. Until Spring 2022!





ICC FraudNet
Global Annual Report 2022

PART ONE

CRIMINAL AND CIVIL DEVELOPMENTS IN FRAUD AND ASSET RECOVERY

The Interaction of Criminal and Civil Process in Fraud Cases

Stephen Baker

Abstract

In this article, Stephen Baker, a Senior Partner at Baker and Partners, considers the interaction between criminal and civil process in cases involving fraud. He explores the operation of both criminal and civil regimes in this area, the interaction between professionals therein, and promotes a pressing need for greater collaboration between the two frameworks if the goal is to maximise asset recovery, particularly in cases with cross-border elements.

Introduction and Background

1. In most functional jurisdictions, the facts which constitute a fraud tend to be a crime. Fraud also tends to be a civil wrong. A person deceived by fraud is the victim of a crime. That person is also the victim of a civil wrong. The victim has the option of reporting a crime to the law enforcement authorities with a view to the perpetrator being brought to justice and obtaining compensation. The victim also has the option of issuing proceedings in the civil courts so as to seek redress. Given that the victim is the same person whether or not the proceedings which are brought are criminal or civil, the two processes should run in harmony. Sadly they presently do not seem to do so.
2. Lawyers who specialise in fraud tend to fall into opposite camps. Criminal lawyers who are almost overwhelmingly servants of the state favour the criminal process. Investigation. Prosecution. Confiscation. Compensation. Mutual Legal Assistance Requests to obtain evidence and criminal freezing orders abroad. By comparison, specialist fraud lawyers in private practice almost all seem to favour the civil process. The standard of proof is lower. Balance of probabilities/preponderance of the evidence is a lower standard than the criminal standard of 'beyond reasonable doubt'. Evidential rules are almost inevitably less strict. Keep control of the case. Don't let the state take over through criminal process. The state will force the civil case to halt while the criminal process takes its course. If you invite a bear to a picnic do not be surprised if it eats all the sandwiches. Civil process allows the facilitators of fraud to be held accountable. Worldwide freezing orders and third party

disclosure orders and the appointment of liquidators and other Insolvency Professionals are the only true way forward.

3. Criminal prosecutors and law enforcement agents appear to be suspicious of private lawyers acting for the victims of fraud. The private lawyer is in this to make a profit for himself. He is not really interested in helping his client just enriching himself. If the lawyer is from a big international firm there is a further suspicion that the same firm acts for bad guys and not just victims.
4. Private lawyers are suspicious of prosecutors. Myths and generalisations abound. If the state confiscates assets they keep them all for themselves. The state does not pay assets seized and confiscated to the victims. The state anyway does not have the interest, resources, expertise or perseverance to follow the evidence wherever it needs to be followed.
5. This distrust where it exists needs to be dispelled because in order to properly combat fraud and to give victims the best chance of securing justice, the criminal and civil systems need to co-exist and work hand in hand to ensure fraudsters are held to account and victims properly compensated.
6. It is sadly true that in many cases of fraud there will not be a meaningful criminal investigation. Fraudsters have overwhelmed the resources of the state to effectively combat it. There are insufficient resources and insufficient expertise within law enforcement authorities throughout the world. Frauds are often committed by criminals using multiple jurisdictions. Money or value is transmitted quickly away from the victim at the press of a button and then dispersed through multiple jurisdictions.
7. In some cases there will be meaningful criminal investigations and potentially prosecutions. In some instances there will be the opportunity for the state to use non-conviction based forfeiture remedies.
8. In all cases of fraud there will be the possibility of using civil remedies. In the vast majority of fraud cases there is no good reason for law enforcement and private lawyers not to work together constructively with a view to ensuring a remedy for the victim of fraud. In multi-jurisdictional cases, it is essential that they do so.

Terminology

This article will refer to three principal methods of asset recovery and securing financial redress. Two of them will be considered as criminal process. First, the prosecution and sentence of a person following criminal conviction. Second, non-conviction based forfeiture whereby property is seized by the state as representing the proceeds of crime. Third, and in contrast, civil proceedings where a person privately sues another for return of property or damages or the equivalent for harm done to him or her.

Some Case Studies

Which Route(s) Should a Victim Choose?

1. In many cases, and particularly in major international frauds, all three principal methods of dealing with fraud namely criminal prosecution, non-conviction based forfeiture and civil proceedings will be available and likely should be used. Proceedings emanating from the scandal surrounding the Malaysian sovereign wealth fund '1 MDB' are a good example of the use of multiple methods of securing redress. There has been a criminal prosecution and conviction of the former Prime Minister in Malaysia, as well as criminal proceedings underway in Switzerland. The United States Department of Justice has used non-conviction based forfeiture to great effect where some USD \$750 million of assets has been recovered. There are also civil claims underway in various jurisdictions. A third party facilitator, Goldman Sachs, has faced criminal, regulatory and civil proceedings and has paid, or will pay, over USD \$3 billion to the victim.
2. How then can the criminal and civil processes work together? How does a victim choose which route to take?
3. Every case is of course fact specific. A client's resources to fund proceedings can be an important factor - though the potential availability of third-party litigation funders has altered that dynamic. If the state has the resources and the will to deal with a fraud, then it is the taxpayer of the state who meets the bill not the victim. That can of course be a very important factor.
4. In the notorious *Abacha* proceedings, only the criminal process was used and with great skill and success. It is, however, an unusual case substantially driven by private lawyers in Geneva instructed by Nigeria. Well over \$2 billion was recovered over the course of some twenty years by way of criminal process, including non-conviction based forfeiture. With regards to large amounts

recovered, the overwhelming likelihood is that recoveries would have been much quicker by use of civil process - but there is no doubting the effectiveness of the steps taken.

5. In the case of the corrupt former Mayor of Sao Paulo, Paulo Maluf, civil proceedings were issued offshore on the British Crown Dependency Jersey against two British Virgin Islands ('BVI') companies which were complicit in his fraudulent conduct¹. Those companies were held liable after trial. The judgment against them is in the process of being enforced through the appointment of liquidators over those companies. Maluf was also sentenced to a term of imprisonment in Brazil following criminal conviction.
6. In the case of *Windward Trading*,² this offshore company was prosecuted for money laundering and a confiscation order made against it. The proceeds of criminal conduct in Kenya had been laundered through it for many years. It still held assets. It would have been possible to issue civil proceedings against it but resources were an issue. The directors of Windward Trading were financial services professionals based offshore in Jersey. Jersey has a strong financial services regulator which demands the very highest standards of its regulated community. The company pleaded guilty to money laundering. The assets held by it were confiscated and returned to Kenya.
7. There are of course multiple examples of the use of civil process to secure redress. A common and very good reason for choosing civil process will be with a view to holding third party facilitators (such as banks, lawyers, accountants and other professionals) who facilitate fraud liable for their misconduct. These persons potentially have the resources to pay damages awarded by courts where otherwise assets have been lost because they have been dissipated.
8. Victims of fraud should not see the use of civil and criminal process as a binary choice. Very often it will be important to use both processes.
9. By way of example in the *Maluf* case referred to above, there were criminal investigations in Brazil, Jersey and the United States. Funds had been laundered from Brazil to New York then to Jersey. There was cooperation between the law enforcement authorities in the three jurisdictions. This by way of MLAT. This led to a Red Notice being issued on behalf of the United States in relation to Maluf and his son. It resulted ultimately in Paulo Maluf's

¹ Brazil v Durant [2012] (2) JLR 356 [2015] UKPC 35

² AG v Windward Trading: [2016] JRC048A

criminal conviction in Brazil. It did not however result in any or any substantial financial redress to the victim, which was the municipality of Sao Paulo.

10. Financial redress was obtained by the issuing of civil process in Jersey and by the appointment of liquidators over the BVI companies against whom a civil judgment had been obtained. Assets were frozen in offshore bank accounts first by the use of criminal process and then by civil freezing orders, the criminal and civil processes working hand in glove.
11. In this case, much of the evidence used in the civil proceedings in the trial offshore was the same as that used in criminal proceedings in Brazil. That is in large part because much of it came from the victims of the fraud - namely the municipality of Sao Paulo. The documentary and other evidence which originated offshore for use in civil proceedings was obtained by third party disclosure orders made by the Jersey court against local financial service providers.
12. The criminal and civil processes thus worked in harmony in that case as they should have. The case is a good example of the criminal and civil process working together to secure a just result. It sadly seems all too rare, even though the case itself provided uniquely invaluable and expedited experience in the techniques now being discussed.

Freezing Assets

13. Criminal process can allow assets to be frozen quickly. Offshore financial centres have their own laws and procedures which govern when suspicious activity reports ('SAR') must be made by financial service providers and the legal consequences of making such a report. In Jersey, Guernsey and the Isle of Man, if an SAR is made then unless a police officer consents to the account (if it is a bank which made the SAR) operating normally, then the financial service provider and the relevant bank employee runs the risk of being prosecuted for money laundering. There is no time limit on the police officer's refusal of consent. Thus a very effective and cost effective step for the victim of a fraud can be to communicate with the bank and or law enforcement with a view to the generation of an SAR and consequent blocking of the account by way of no consent.
14. It will be understood that even where a victim has decided that a freezing order must be obtained in civil proceedings, it can often be most useful to have used a criminal complaint to ensure funds are frozen and not dissipated while the civil application is perfected.

15. The answer as to whether to engage with the law enforcement authorities so as to ensure the freezing of assets will be jurisdiction specific. What may be possible in one jurisdiction may not be possible in another.
16. The decisions in this regard are not straightforward and require particular knowledge and expertise. It is essential that a lawyer is instructed who is very familiar with the different models of the various means of obtaining evidence and freezing assets, using both criminal and civil methods in multiple jurisdictions.

Obtaining Documents and Other Evidence

17. In the common law world there are a variety of method of obtaining documents and evidence for use in civil claims or potential civil claims. At the early stages, these may include third party disclosure orders often referred in the British-influenced spheres as Norwich Pharmacal or Banker's Trust orders after the cases which established the precedent for them. In such a case, a bank might be ordered to disclose information to allow a victim of fraud to discover the identity of the fraudster or trace assets stolen from him or her. In very strong cases, search orders can be obtained even in a civil claim. After civil proceedings are issued, witness summonses/ subpoenas can be issued from those who hold relevant material. Discovery where a party has to disclose material which might harm its case, as well as that which helps it, has to take place. Evidence from abroad can be sought by way of letters of request, usually authority to authority.
18. In many civil law jurisdictions, such remedies and orders are not available in civil proceedings. Thus there effectively has to be engagement with the criminal process in order to progress the case and secure redress. By way of example, in Switzerland the victim of a fraud can make a criminal complaint to the law enforcement authorities. If criminal proceedings are instigated, then he or she can apply to be joined as a civil party to those proceedings. This is not the place to describe such process in detail - save to say that this is a very powerful tool which can lead to the powers of the state being used to freeze assets, obtain access to the evidence, and to make submissions as to how the investigation should best proceed. At the end of any trial, or if proceedings are settled, there is the prospect of a victim being compensated.
19. In some offshore centres it may be wise to engage with the law enforcement authorities with a view to securing and obtaining documents and other evidence. It would be a mistake to consider all offshore centres as the same. The regulation of some centres is more advanced than others. The judiciary in some centres may be more willing to assist parties to civil claims than others.

Their legislation varies considerably. It will often be wise to give the closest consideration to engaging with law enforcement. It may be that a victim of fraud may have invested in a purported fund or hold shares in an offshore company. Those investments may give the victim legal rights to certain information. The rights as a shareholder, or the contractual rights in a fund, will impose basic obligations on the fund or company to provide documents and other information. By contrast, the law enforcement authorities will often have the right to obtain all documentation and information relevant to the fraud both hard copy and electronic. In the right case having the law enforcement authorities seize all relevant material can be of particular comfort and importance.

20. The next step is to consider how that material might be obtained from possession of the law enforcement authorities. There are a variety of ways of approaching this. Ideally law enforcement should take witness statements from victims of fraud and ask them whether they were aware of certain facts and information. They should ask what they would have done if they had known about certain facts and matters. As a by-product of the criminal investigation, information which the victim can use in civil proceedings is brought to their attention.
21. The present reality is that in many jurisdictions there is still hesitation in the disclosure to victims by law enforcement of material generated in criminal proceedings. It is drilled into police officers that information which they obtain in criminal proceedings can only be disclosed for the purposes of criminal investigations. That principle is generally correct and there is said to be a strong public interest in information provided to law enforcement during a criminal investigation remaining confidential and only being used for criminal purposes and in criminal proceedings. There is of course also a strong public interest in the victim of fraud being compensated for the dishonest conduct they have suffered. The answer to the tension which these competing public interests cause is jurisdiction specific. It may be that in some jurisdictions it is not difficult to obtain the key information needed. Would anybody really suggest a police officer could not tell the victim of a burglary that his flat screen tv and computer had been recovered from a known burglar's garage? Why is the principle different where it is funds transferred into a bank account as a result of fraud?
22. In other jurisdictions there may be relevant statutes which prevent disclosure of information other than in the course of a criminal investigation. In such circumstances a court order may be needed to allow law enforcement to provide documentation or other information to the victim of fraud. In some jurisdictions it will be straightforward to have law enforcement not resist a

summons or subpoena issued by the local court to provide such material. In others it will be much more complicated.

Recovering Assets/ Securing Damages or Compensation

23. Assets can be recovered and compensation awarded in the criminal process. In the common law world, it would be rare that a criminal prosecution would offer a victim of fraud the best chance of recovery. The civil process would usually be much the simpler and better course mainly because the standard of proof is so much easier to meet. In civil law jurisdictions, the advice generally given is that it is the criminal process which gives the best chance of proper financial redress. As always, the answer to the best route is fact and jurisdiction specific. By way of further example, some offshore centres have legislation which allows funds held in bank accounts to be subject to non-conviction based forfeiture. A victim can be made party to these applications. In many circumstances this legislation essentially means that the evidential burden is on the account holder to show the funds held are not the proceeds of crime. This can be very difficult for the wrongdoer and so this route is potentially very powerful.
24. In some cases, such as 1 MDB referred to above, it may well be that there will be a criminal prosecution in one jurisdiction, civil proceedings in others, and non-conviction forfeiture applications in yet others. Keeping an open mind to the best route is crucial.

Good Will

25. Where the victims of fraud need the assistance of law enforcement authorities, it is necessary to generate good will. Law enforcement tends to be short on resources. Fraud is endemic and the authorities must feel that they are forever chasing their tail. On a practical level it is thus important to give them as much help as possible. Providing them with good and full witness statements, chronologies, dramatis personae, and structure charts is essential. Putting the documents in a chronological and comprehensible order and identifying the key ones is inevitably important.
26. Law enforcement has access to a wide range of information which it can obtain both domestically and from abroad by way of production orders, MLATS and legislation which allows information to be shared with overseas colleagues. That does not mean that it will not welcome the assistance of victims and material generated by it. Different jurisdictions will have different levels of experience of dealing with fraud - particularly multi-jurisdictional fraud. Also, it is worth repeating that resources is an issue.

27. By way of example, if during the civil process subpoenas are obtained in the United States under USC 28 1782, which enables US district courts to order witnesses within the district to produce evidence and information for use in proceedings or potential proceedings abroad, consideration should be given to articulating that the material will be used in both civil and criminal processes. Good will can be generated by producing such material which could include key evidence such as bank transfers or the identity of the beneficial owner of a property.
28. In many ways it is a matter of common sense that if ultimately there is a discretion on law enforcement as to whether to voluntarily provide a victim of fraud with information or whether or not to resist a witness summons, then if the victim has done everything she reasonably can to assist the criminal investigation, then the prospect of a discretion being exercised in her favour is substantially increased.
29. Where good will is generated, then the prospect of reaching an understanding and agreement as to the sharing of information increases.

Conclusion

In multi-jurisdictional fraud cases, particularly those involving offshore centres, it is almost inevitable that there will have to be engagement between private lawyers instructed in civil proceedings and law enforcement authorities if the chances of recovering assets or damages are to be maximised. It should be to the benefit of all that there is co-operation. Local and international legislation will have to be navigated so as to enable full co-operation. This is a new and developing area and there is reason to be cautiously optimistic that there is a growing understanding of the merits and best techniques of such co-operation.

About the Author

Stephen Baker is an English barrister (1989), Jersey Advocate, and Senior Partner at Baker & Partners. He is called to the bar of the BVI. He is an expert in the recovery of assets and the award of damages in corruption cases, and on the interaction between the civil and criminal law in fraud cases including those seeking to evade judgment debts. He specialises in complex international financial litigation including trust and commercial disputes as well as civil fraud.



He is currently Lead Counsel in a multi-billion dollar global asset recovery claim. Stephen regularly acts for foreign governments in asset recovery actions. Most notably, he has been retained on behalf of the Federal Republic Nigeria in the asset recovery action as regards former President Sani Abacha. He acted for the Federal Republic of Brazil in its first substantial asset recovery action outside of the jurisdiction seeking the recovery of assets held through an offshore unit trust held to the benefit of a senior Brazilian politician. He has also acted for the Islamic Republic of Pakistan re Bhutto, Zardari, Minwalla and others, and for the Kenyan Ethics and Anti-Corruption Commission re Guchuru and Windward Trading.

He has been responsible for the strategies which have led to the recovery of many hundreds of millions of US dollars to victim states. Between 2017-2019 he was Chairman of the IBA Anti-Corruption Subcommittee on Asset Recovery. Stephen was a member of the FATF style review team, carried out by the OFGBS on Gibraltar and has advised a very substantial non-European state on its FATF requirements. He was a member of the Jersey team that responded to a FATF review, and is frequently instructed as a reporting professional in regulatory matters focused particularly on financial institutions' AML/CFT procedures.

Stephen is also regularly instructed by the Attorney General of Jersey in the most complex criminal cases. In 2016, he was named the ACTAPS Offshore Contentious Trusts Practitioner of the Year. During 2018 and 2019, Stephen was the Chairman of the IBA Asset Recovery Subcommittee. He is the Chairman of the Institute of Law in Jersey. Stephen works regularly with the World Bank Financial Market Integrity Division, including the Stolen Asset Recovery Initiative most recently on the publication of 'Going for Broke - the Use of Insolvency Tools in Corruption Cases' (Dec 2019).

He regularly participates in a wide variety of international events organised by the ABA, IBA, Offshore Alert, KNect365, Florida University College of Law, IBRA, ICC FraudNet and the University of the Western Cape. He spoke at the UNCAC conference for state parties in Abu Dhabi, the UNCITRAL Colloquium on asset tracing and recovery tools in Vienna and participated in the Global Forum for Asset Recovery (GFAR) in Washington DC and at UNGASS 2021.

Contact Stephen Baker: T: +44 (1534) 766254; E: stephenbaker@bakerandpartners.com

Evaluating Different Unexplained Wealth Orders (UWOs) and Explaining their Effectiveness

Diane Bugeja & Peter Mizzi

Abstract

In this article, Diane Bugeja, Senior Associate, and Peter Mizzi, Compliance and AML Advisor at Camilleri Preziosi Advocates, compare the differences between Unexplained Wealth Orders ('UWOs') found in Ireland and the United Kingdom ('UK'). They examine factors that have led to UWOs' effectiveness in some jurisdictions, in comparison to others and cite legal challenges and difficulties that have arisen through case law. Finally, they discuss the ongoing legal developments in the Maltese jurisdiction with regards to the recently enacted Proceeds of Crime Act that has omitted the inclusion of UWOs.

Introduction

Although not new in some countries, UWOs are gaining traction in several jurisdictions. UWOs are an investigative tool that empowers authorities and enforcement bodies with the right to confiscate assets that they believe derive from illicit activities, so called non-conviction-based asset ('NBA') confiscations. NBA confiscations have a clear advantage over post-conviction-based confiscation. Namely, the respondent need not be convicted of a crime. Investigative authorities can apply for a UWO if reasonable grounds exist to suspect that the property in question does not fit the known economic customer profile.

In contrast to a criminal conviction, enforcement bodies such as the National Crime Agency ('NCA') in the UK are not required to prove that the individual illegally obtained the property in question, but rather the burden lays on the respondent to prove legitimate acquisition. Therefore, the purpose of an UWO is to deal with the issue of financial crime from a different perspective by investigating and challenging individuals who own assets that appear disproportionate to their known income. This article will discuss the successes and limitations of the tool as well as when and how they should be used by authorities.

Civil forfeitures in Ireland

Despite falling under a different name, civil forfeitures in Ireland are widely regarded as a success story. Becoming the first European country to introduce the system in 1996, it is often considered the best model¹. Following the murders of a journalist and a policeman at the hands of organized criminals², the Irish government worked swiftly towards enacting the Proceeds of Crime Act (1996) ('POCA') and subsequently introduced the new agency tasked with enforcing the legislation, The Criminal Assets Bureau ('CAB').

The Irish model has largely been considered a significant success and despite some reservations made by the Financial Action Task Force ('FATF')³ concerning the actual amounts retrieved, evidence points towards crime reduction, particularly in the first five years of the POCA. Albeit, it is alleged that criminals have instead relocated elsewhere in Europe and newly organised crime groups still emerged⁴. Whilst this can be considered a win for Ireland, criminals are increasingly seeking alternative arrangements which highlight the limitations in this aspect.

The POCA⁵ allows for members of the CAB to make an application to the courts, should the following criteria be met:

- a) That a person is in possession or controls of:
 - i) specified property and that the property constitutes, directly or indirectly, proceeds of crime, or
 - ii) specified property that was acquired, in whole or in part, with or in connections with property that, directly or indirectly, constitutes proceeds of crime,

and;

- b) that the value of the property or, as the case may be, the total value of the property referred to in both subparagraphs i) and ii) is not less than €5,000.

¹ King, C. 'Civil Forfeiture in Ireland: Two Decade of the Proceeds of Crime Act and the Criminal Assets Bureau', April 2016 available at <http://www.dsps.unict.it/sites/default/files/Civil%20forfeiture%20in%20Ireland%20-%202%20decades.pdf> accessed 15 October 2021.

² In June 1996, journalist Veronica Guerin was murdered by a criminal gang, whereas Detective Garda Jerry McCabe was murdered by members of a terrorist group

³ FATF, Mutual Evaluation Report on Ireland, September 2017 <https://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-ireland-2017.html>, accessed 15 October 2021

⁴ Groups of States Against Corruption, "Second Evaluation Round, Evaluation Report on Ireland," 2005 <https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=24507&lang=en>, accessed 15 October 2021

⁵ Proceed of Crime Act, 1996 At: <http://www.irishstatutebook.ie/eli/1996/act/30/enacted/en/print.html>, accessed 15 October 2021

When compared with other jurisdictions such as the UK, the legislation has been set out in a manner that makes it simpler and more convenient for authorities to confiscate assets. The value threshold was recently reduced from €13,000 to €5,000, expanding the scope of targeted properties and is a possible factor leading to more confiscations in the case of smaller items such as luxury goods and jewellery.

The POCA has some key features:

- retrospective powers to any property;
- no requirement to identify the predicate offence;
- belief or hearsay evidence is permissible at court;
- reverses the burden of proof to the respondent.

Despite no intent in targeting the proceeds derived from offences in other states, the POCA was revised in 2005 to include the proceeds of foreign offences that were held at any time in Ireland.

The CAB is made up of officials and officers from several agencies such as, *inter alia*, the Garda Síochána, Department of Justice and Revenue Commissioners. This centralised model increases the flow and sharing of information and resources, which is crucial when conducting investigations. The interconnectedness of the agency has been deemed as the main reason for its outstanding success⁶.

The CAB multi-agency simply needs enough ‘belief evidence’ or reasonable grounds to suspect that property has derived from criminal activities, to proceed with an application for an UWO. The 2019 CAB annual report⁷ confirmed that there was a substantial increase in the number of assets frozen, a record high of €64,985,550.30. This was mainly attributed to a large freezing order over the popular cryptocurrency, Ethereum.

Irish case law - civil or criminal in nature?

The POCA has endured challenges over its constitutionality. Despite this, it has maintained consistent application since its implementation. It is widely argued that civil forfeitures are intrusive and create inequality between the respondent and

⁶ Booz Allen Hamilton, Comparative Evaluation of Unexplained Wealth Orders, January 2012, <https://www.ojp.gov/pdffiles1/nij/grants/237163.pdf>, accessed 15 October 2021

⁷ Criminal Assets Bureau Annual Report, 2019, http://www.justice.ie/en/JELR/CAB_Annual_Report_2019.pdf/Files/CAB_Annual_Report_2019.pdf, accessed 15 October 2021

investigative authorities. In fact, several countries have held back from introducing the key functions of POCA, such as the reversal of the burden of proof - claiming that it violates fundamental human rights such as the presumption of innocence and due process. The consistent debate here revolves around whether civil forfeitures are *truly* civil or are they disguised as civil, but rather are criminal proceedings without constitutional protections.

Attorneys in the case of *Murphy vs. GM PB PC Ltd [1999] IEHC* argued this in the Irish High Court. However, the court concluded that proceedings under the POCA are *in rem*⁸ rather than *in personam*⁹. Therefore, actions are taken against the property in question - whereby the respondent is required to restore or resolve such a situation. As opposed to criminal proceedings, civil proceedings do not impose a fine or punishment on the respondent.

The cases of John Gilligan have spanned over the past 20 odd years, including a total of 29 appeals. In particular, *Gilligan vs CAB 1997 No. 1667P* raised comparable claims surrounding the constitutionality of the legislation. The court again maintained consistency, refuting the claims and reiterating that forfeitures instituted under the POCA are strictly civil in nature.

Therefore, it can be concluded that whilst valid arguments do exist for the presumption of innocence and other constitutional rights under criminal law - these simply do not apply to proceedings issued against respondents by the CAB, as no criminal punishments arise.

Nonetheless, respondents and their lawyers have sought to challenge the law, claiming that in reality it is a criminal law and thus enabling protection under the law and constitution.

UWOs in the United Kingdom

As per the Criminal Finances Act 2017¹⁰, the High Court must be satisfied that there is reasonable cause to believe that—

- a) the respondent holds the property, and
- b) the value of the property is greater than £50,000.

⁸A Latin term meaning “against a thing”

⁹A Latin term meaning “against a person”

¹⁰ Criminal Finances Act, 2017

<https://www.legislation.gov.uk/ukpga/2017/22/part/1/chapter/1/crossheading/unexplained-wealth-orders-england-and-wales-and-northern-ireland/enacted>, accessed 15 October 2021

Furthermore, the High Court must be satisfied that there are reasonable grounds for suspecting that the known sources of the respondent's lawfully obtained income would have been insufficient for enabling the respondent to obtain the property.

The High Court must be satisfied that—

- a) the respondent is a politically exposed person ('PEP'), or
- b) there are reasonable grounds for suspecting that—
 - i) the respondent is, or has been, involved in serious crime (whether in a part of the United Kingdom or elsewhere), or
 - ii) a person connected with the respondent is, or has been, so involved.

In comparison with civil forfeitures, UWOs in the UK are more restrictive and focus heavily on foreign PEPs and their close associates. The threshold is also set much higher and the overall wording is more objective rather than subjective as per the Irish model, ultimately narrowing the scope and hindering investigations. Most UWOs in the UK have involved high-value properties of wealthy individuals, attracting media attention and leading to mixed results. Like the Irish model, English law has retrospective powers, meaning that properties acquired before the legislation came into force are still at risk of seizure.

UWOs have an international and extraterritorial reach. A respondent does not need to be a UK resident, and property can be located outside the UK. UK enforcement authorities may seek assistance from the foreign government of the country where the asset is based to enforce an UWO. However, issues encountered include the unwillingness of foreign authorities to assist with enforcing UWOs.

Overall, UWOs in the UK have rarely been used and law enforcement bodies have instead opted for account freezing and forfeiture orders¹¹. As reported by the Organised Crime and Corruption Report Project ('OCCRP')¹², only the NCA has applied for an UWO, even though all agencies¹³ that fall under the National Economic Crime Centre ('NECC') have the necessary powers to do so.

¹¹ Jonathan Watson, *Anti-corruption: unexplained wealth orders struggle to live up to the hype* <https://www.ibanet.org/article/744063A6-DE55-44C4-A74F-EDFF07173EC4>, accessed 15 October 2021

¹² Will Neal & Ilya Lozovsky, Explaining the U.K.'s "Unexplained Wealth Order" <https://www.occrp.org/en/what-is-unexplained-wealth/explaining-the-uks-unexplained-wealth-order>, accessed 15 October 2021

¹³ See: <https://www.nationalcrimeagency.gov.uk/what-we-do/national-economic-crime-centre>, accessed 21 October 2021 - Consisting of the National Crime Agency, Serious Fraud Office, Financial Conduct Authority, City of London Polic, HM Revenue & Customs, Crown Prosecution Service and the Home Office

This suggests that there is not enough incentive, knowledge, or investigative capabilities possessed by the other agencies. Further highlighting issues in the UK, a recent report by the House of Commons¹⁴ had to say the following:

“Available from January 2018, the use of UWOs has been limited so far, having only been obtained in four cases as of December 2020. There have been high-profile successes and failures.

A Government money laundering risk assessment concluded in December 2020 that money laundering has probably increased since 2017, suggesting that UWOs are yet to have the desired impact.”

Although still in the early days of the UWO regime, the UK’s framework does not appear to have fully taken off yet. A factor that may be limiting UK enforcement agencies’ capacity is the high threshold (£50,000) when compared with the Irish model. It might be the case that the legislation encourages agencies to focus too much on foreign PEPs which, although maybe of higher risk in terms of tracing their assets, is a more burdensome task. This is especially so when dealing with uncooperative foreign jurisdictions.

Further, the NCA has so far only utilized this tool in relation to high-value UK residential properties, even though it has powers over and beyond its territorial waters and has disregarded other high-value items such as luxury vehicles, yachts, designer goods etc.

Has the *Baker* legal defeat shattered confidence in the UK?

UK ministers promoting the law had big predictions for the impact of UWOs, with the Home Office estimating costs of only £10,000 for each case and a total of 20 per annum. Expectations were that the funds recovered from proceedings would be over and above any minor costs. The things unfolded couldn’t be further from projections. A major contributor to the financial loss and consequent lack of confidence in the UWO regime was following the crushing legal defeat in the *National Crime Agency vs Baker (2020) EWHC 822 (Admin)*.

The High Court granted the NCA three UWOs and related IFOs in respect of three properties whose registered owners were offshore Private Interest Foundations (‘PIFs’). The respondents managed to dismiss the orders brought against them, based on the following:

¹⁴ Ali Shalchi, Unexplained Wealth Orders, *House Of Commons*
<https://researchbriefings.files.parliament.uk/documents/CBP-9098/CBP-9098.pdf> , accessed 15 October 2021

- i) Errors of law and approach by the NCA in the application of the requirements for the making of a UWO;
- ii) Material non-disclosure by the NCA to the Judge at the *ex parte* hearing and inadequate inquiry by the NCA. Judgment Approved by the court for handing down;
- iii) The orders were sought and made on a flawed basis, lacking the necessary investigative groundwork required that would have established certain facts.

The NCA alleged that the properties belonged to a former Kazakh PEP, Rakhat Aliyev. It was believed that the properties were bought with the proceeds of his crimes in Kazakhstan and that his family subsequently laundered the funds through the properties. The Court concluded that the NCA failed to identify the following facts:

- i) Aliyev's family (specifically his ex-wife and son) were separately wealthy of Rakhat and had sufficient funds to purchase the properties;
- ii) Had the NCA conducted thorough research into crimes brought against Rakhat in 2008, they would have identified that his assets were seized and therefore the properties in question were unrelated;
- iii) The NCA failed to meet the UWO threshold requirements concerning reasonable cause that the respondents held the properties, reasonable grounds to suspect that the properties were illegally obtained and reasonable grounds for believing the PEP or serious crime requirements were met.

As a result of the defeat, the legal penalty amounted to a third of the NECC's annual budget, £1.5 million.

The future of UWOs in the UK is uncertain. Following the failure in the above case, one can expect that the NCA will be hesitant yet very careful when picking its next target, ensuring that their homework is sufficient beforehand. The fundamental legal failure here was a lack of sufficient initial investigation and somewhat 'jumping to conclusions'. Furthermore, the NECC should take this particular case as a lesson learned. Going forward, one would expect to see the NECC enhance its investigatory research, knowledge, and resources, whilst also encouraging other authorities that form part of the committee to pursue UWOs. The NECC should see this as an opportunity for growth and a better understanding of how and when the tool should be used.

Once dubbed as a silver bullet in the fight against financial crime, UWOs in the UK are now at a critical juncture - are authorities confident enough to pursue new cases or has the confidence been shattered? The latter seems to be more prevalent since the *Baker* judgement, no authority has pursued an UWO.

On the other hand, NCA vs Hussain [2020] EWHC 432 (Admin), was the first successful UWO that led to the recovery of assets from an individual. Mansoor Hussain was ordered to hand over £9.8m in assets, mainly consisting of property. The court concluded that Hussain qualified under the “Serious Crime Requirement”, whereby he was accused of being a professional money launderer. The case was described as a ‘milestone’ by the director general of the NECC. Therefore, authorities have the capabilities to successfully pursue UWOs, and the success of UWOs is currently in the balance.

Legal developments in Malta

There have been many recent and ongoing developments in Malta. The recently-enacted Proceeds of Crime Act in Malta has stirred up some controversy and debate amongst members of Parliament. The main objective of the POCA (Act No. V 2021, of the Laws of Malta), is to provide the Asset Recovery Bureau (ARB) with the ability to act without the need for a criminal conviction - similar to legislation in Ireland and the UK.

As the law currently stands, the ARB can only confiscate assets once all criminal proceedings are finalised. The law also currently states that the ARB needs to start criminal proceedings and must prove beyond a reasonable doubt in court that such assets were generated through the proceeds of crime.

Under the act, the ARB will retain its current function but can also institute civil proceedings to confiscate assets based on reasonable suspicion. The proposed law seeks to fast-track confiscations and make it easier for Malta’s authorities to clamp down on money laundering.

Controversially, however, there are only three instances when this may occur: where the perpetrator flees or is not in Malta; where the perpetrator is dead; or when the perpetrator dies prior to the conclusion of the criminal proceedings. At no given time when the perpetrator is alive, or is in Malta, can such proceedings take place. A specialised civil court will be created to deal with asset recovery.

Additionally, the act, does not include provisions for UWOs - a move that was expected and is fiercely criticised by members of the opposition party. The Maltese government has claimed that certain unexplained wealth clauses exist currently in tax and social security laws and that UWOs will only be considered as a second step.

In terms of Article 14 of the Income Tax Management Act (Chapter 372 of the Laws of Malta) when:

“the Commissioner For Revenue has reasonable grounds to suspect that tax has been, is, or maybe evaded, he may request, by notice in writing to a

designated person, that the designated person provide the Commissioner within the time indicated in such notice not being less than thirty days from the date of service of such notice, with all such information and documentation which the designated person may have relating to property of any kind or description, transferred or delivered to him by that person and owned, possessed, or held by the designated person under any title on behalf of or for the benefit of any such person on the date of the said notice or during the period specified in such notice not commencing earlier than five years from the date of such notice; provided that the designated person shall not be bound to provide information to the Commissioner in respect of any beneficiaries for whose benefit the property may be held or the terms and conditions under which it is so held.”

This clause confirms that whilst such clauses in relation to unexplained wealth do exist, they are limited to tax laws and the Commissioner for Revenue. This essentially disregards other authorities and narrows the focus on tax crimes. Whereas the inclusion of UWOs in the Act would extend powers to all enforcement bodies, and in an ideal scenario lead to more confiscations.

Concerns were raised by a member of the Maltese opposition,¹⁵ who emphasized that the then Bill should not merely be geared towards passing the Moneyval test or aligning with the Venice Commission’s requirements, but “should be instruments of change which contribute to the common good of our society.”

Recent statistics show that the ARB recovered a small amount of €1,500 in August 2018 and €1,260 in October 2018¹⁶. Considering these low numbers, exclusion of UWOs and the poor track record, it is seemingly unlikely that Malta will see a significant increase in asset confiscations.

Conclusion

UWOs can be a powerful tool that law enforcement authorities can make use of. As we’ve seen above, the success in different jurisdictions is determined by several factors, including how the legislative frameworks are set out, the thresholds set, and efficient collaboration between the agencies tasked with implementing the law.

Factors such as reversal of the burden of proof should make the process less troublesome for investigators and therefore should be a favourable approach when tackling financial crime. As seen with the multi-agency approach in Ireland, sufficient investigation, collaboration, and interdependency is an effective policy.

¹⁵ See: <https://timesofmalta.com/articles/view/opposition-urges-introduction-of-unexplained-wealth-orders.823852> , accessed 20 December 2021

¹⁶ See: <https://timesofmalta.com/articles/view/asset-recovery-bureau-recovers-2760-in-criminal-assets.697040> , accessed 20 December 2021

Only then may we finally see an increase in confiscations in the UK and hopefully in Malta, should UWOs be introduced in the near future.

However, as seen in *Baker*, the reversal of the burden of proof does not absolve authorities from conducting the necessary initial research. Aside from the Hussain case, forfeitures in the UK have been few and far in between, thus, one begins to question whether UWOs are indeed an effective tool or have legal challenges disrupted the flow and discouraged enforcement authorities? Of course, we will gain a clearer picture of success once the ongoing cases are concluded.

To sum up, the effectiveness of UWOs varies depending on the jurisdiction, whether there are sufficient enforcement efforts and the confidence of authorities. It remains to be seen whether UWOs in the UK are indeed effective or not, considering the minimal amount of UWOs pursued and whether legal developments in Malta will increase asset confiscations despite the omission of UWO legislation.

About the Authors

Diane Bugeja practices primarily in financial services law, financial regulation and anti-money laundering regulation, providing advice to local and overseas clients on the impact of the current and forthcoming regulatory regime on their business models. Diane also advises clients on the regulatory aspects of a wide range of transactions, including licensing-related matters, capital markets initiatives and on-going liaison with regulatory authorities more broadly. Diane joined the firm as an Associate in 2016 and was promoted to Senior Associate in January 2017. She was previously a risk and regulatory consultant at a Big Four audit firm, working in Malta and in London, and subsequently joined the enforcement departments of the UK and Maltese financial services regulators. Diane successfully completed her PhD in Law in 2017 at King's College London. She is a visiting lecturer at the University of Malta and is regularly invited to speak at conferences and deliver seminars on various aspects of financial services law and financial crime.



Contact Diane Bugeja, Senior Partner: Camilleri Preziosi Advocates: T: (+356) 21238989; E: diane.bugeja@camilleripreziosi.com



Peter Mizzi works as an advisor at Camilleri Preziosi advising primarily in financial crime and regulatory matters. He has over three years of experience in issues relating to anti-money laundering, terrorist financing, bribery and corruption, fraud, and sanctions. He regularly advises financial institutions and other corporates with their policies relating to financial crime and conducts reviews of client files. Peter also delivers trainings on anti-money laundering and terrorist financing. He has also assisted regulators on the development and implementation of regulations on financial crime issues. Peter holds an International Diploma in Anti-Money Laundering from the International Compliance Association (ICA) as well as a Bachelor of Science degree in Business Administration with International Business from the University of London (UOL). Before joining Camilleri Preziosi, Peter worked at a Big Four audit firm in Malta, where he worked as a senior compliance associate and was extensively involved in one of the largest local remediation projects.

Contact Peter Mizzi, Compliance and AML Advisor: Camilleri Preziosi Advocates: T: (+356) 21238989; E: peter.mizzi@camilleripreziosi.com

Recent Developments in Pursuing Claims Against Organized Crime Group Representatives in Japan

Hiroyuki Kanae & Hidetaka Miyake

Abstract

In this article, Hiroyuki Kanae, and Hidetaka Miyake, Partners at Anderson Mori & Tomotsune discuss recent Supreme Court decisions confirming that the representatives of organized crime groups may be held liable for damages in special fraud cases.

1. Background

Japanese organized crime groups are notoriously known as "Yakuza". In particular, certain groups are well-known around the globe because they have been designated as transnational crime syndicates subject to economic sanctions in the United States ('US') under the International Emergency Economic Powers Act. From the perspective of damage recovery, if a citizen suffers damage as a result of a tort committed by a member of an organized crime group, it is generally difficult for the citizen to obtain an adequate remedy by pursuing a claim against the low-ranking members of the group. Therefore, there have been attempts to claim compensation for damages from the leaders of organized crime groups ('top gangsters') on the grounds of employer's liability under the Civil Code in Japan. In the case of organized crime groups with complex pyramid structures, however, it has been highly difficult to prove the employment relationship between the 'top gangster' and the low-ranking group members who had committed the relevant illegal acts. What makes the issue more complex is that there have been some recent changes in the activities of organized crime groups. In this regard, it is generally understood that there are two types of cases where citizens typically suffer damage from organized crime groups. The first type is where citizens become the target of violence and intimidation by organized crime groups. Another type is where citizens are accidentally injured in confrontational battles between organized crime groups. Recently, however, there have been an increasing number of non-typical cases in which organized crime group members are involved in so-called 'special fraud' (*tokushu sagi*) of which citizens can become victims. In general, special fraud is a

type of crime in which a criminal defrauds a victim of cash or cash cards by claiming to be a relative of that victim or an employee of a public agency.

2. Recent Legal Developments

Against this backdrop, there has been an increase in the number of cases in which victims of special fraud pursue claims for damages against the representatives of organized crime groups under the Anti-Organized Crime Act¹. In March 2021, the Supreme Court declined appeals from some organized crime groups and confirmed two lower court rulings that the representatives of the organized crime groups were liable for damages suffered by victims of special fraud.

In one case, the lower-ranking members of a famous organized crime group named Inagawa-kai deceived four elderly women into paying between JPY 2.5 million and JPY 4 million by pretending to be their sons and saying that they had made their girlfriends pregnant and needed money to deal with the situation. On 16 March 2021, the Supreme Court refused to accept a final appeal from the Tokyo High Court, which ordered the former chairman of Inagawa-kai to pay about JPY16.3 million in damages, and the Tokyo High Court ruling became a final and binding decision on his liability for damages suffered by the victims.

3. Legal Basis

The amended Anti-Organized Crime Group Act, which came into force in 2008, was the legal basis for recognizing the liability of ‘top gangsters’ for damages. Article 31-2 of the Anti-Organized Crime Group Act provides that a representative, etc. of a designated organized crime group shall be liable for any damages arising from the infringement of the life, body or property of another person by a designated member of such designated organized crime group in connection with his/her act of obtaining funds by using force. The meanings of the main terms of this provision are set out in the table below:

¹ The official name of the Anti-Organized Crime Group Act, which was enacted in 1992, is "Act on Prevention of Unjust Acts by Organized Crime Group Members".

| Terms | Meanings |
|---------------------------------------|--|
| Organized crime group | A group that is likely to encourage its members (including members of the group's constituent groups) to collectively or habitually engage in violent unlawful acts and other similar actions |
| Designated organized crime group | An organized crime group designated by the local government authority which is subject to the regulations under the Anti-Organized Crime Group Act |
| Act of obtaining funds by using force | An act of obtaining funds for the maintenance of a livelihood, formation of assets, or execution of business by using force via a designated organized crime group, or an act of obtaining the necessary position to obtain such funds |
| Representative, etc. | A person who represents an organized crime group or a person in a position to control its management |

According to the 2021 White Paper on Police, 24 organizations, including the Sixth Yamaguchi-gumi, Sumiyoshi-kai and Inagawa-kai, are categorized as 'designated organized crime groups' as of 1 June 2021.

The most critical issue in holding a representative of a designated organized crime group liable for damages is whether special fraud falls under the category of 'acquisition of funds by using force'. Since special fraud is typically conducted by telephone or other means without meeting a victim, an organized crime group member usually has no chance to use force against the victim in order to obtain funds. On 4 March 2020, the Tokyo High Court held that, in light of the legislative purpose and the specific language of Article 31-2 of the Anti-Organized Crime Group Act, an organized crime group member is required to 'use' force to obtain funds but this does not mean that he/she is required to 'show' the use of such force to the victim to satisfy the requirement of 'acquisition of funds by the use of force'. In coming to this decision, the court first analyzed and concluded that the legislative purpose of Article 31-2 of the Anti-Organized Crime Group Act is to reduce the burden of proof on victims who seek to recover damages caused by a member of a designated organized crime group through the act of obtaining funds by using force in civil proceedings. The court also mentioned that it is generally difficult for victims to succeed in a claim for employer's liability against representatives of designated organized crime groups under the Civil Code and that low-ranking members of designated organized crime groups, who are usually the direct perpetrators, do not have sufficient financial resources to compensate for the damages suffered by the victims. Secondly, the court pointed out that while Article 9 of the Anti-Organized Crime Group Act prohibits members of designated organized crime groups from

demanding money and other similar conduct by using the specific phrase ‘by showing force’, Article 31-2 of the same Act uses a different phrase: ‘by using force’. In its ruling, the court found that although the relevant organized group member had not shown the use of force to the victims, he had used force to make his subordinate special fraud team members obey his instructions.

4. Collection of Evidence

In Japan, there are no legal procedures like the discovery procedure in the US that can be used to require parties to a dispute to comprehensively disclose relevant evidence. This means that victims of fraud need to collect evidence to allege and prove fraud and damages in civil proceedings. In this respect, it is not easy for victims to gather important evidence, particularly in cases involving organized crime groups. In cases where criminal proceedings are concurrently ongoing, however, it is useful for victims to obtain criminal case records through the procedures for inspection and copying of criminal case records that crime victims are entitled to. Furthermore, after filing a lawsuit, victims can make a petition to the court so that the court can obtain criminal case records from the public prosecutor’s office by issuing (i) a document production request (Article 226 of the Code of Civil Procedure) and (ii) an examination request (Article 186 of the said Code).

In addition, it should be noted that there is a civil case precedent in which no criminal charges were made, but the victims successfully reached a settlement for the recovery of damages. In this regard, in June 2021, Sumiyoshi-kai reached a settlement in which it paid about JPY652 million to victims of cases committed by it, including those cases where no criminal charges were made.

5. Final Remarks

The recent Supreme Court decisions confirming that the representatives of organized crime groups may be held liable for damages on the basis of representative liability under the Anti-Organized Crime Group Act in special fraud cases are expected to significantly advance the civil remedies of citizens who have suffered damages due to the illegal acts of organized crime groups, and to also have a deterrent effect against the illegal activities of organized crime groups in Japan. The Supreme Court rulings are applicable only to special fraud cases, but organized crime groups have recently been engaging in other types of white collar crimes such as market manipulation and black-market financing. The next challenge would be how the Supreme Court ruling can be expanded to apply to such other types of white collar crimes conducted by organized crime groups.

About the Authors



Hiroyuki Kanae is a partner at Anderson Mori & Tomotsune and has more than 30 years' experience in the cross-border litigation. 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.

Contact Hiroyuki Kanae: T. 81-3-6775-1011; E. hiroyuki.kanae@amt-law.com

Hidetaka Miyake is a partner at Anderson Mori & Tomotsune, and 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.

Contact Hidetaka Miyake: T. 81-3-6775-1121; E. hidetaka.miyake@amt-law.com

Who is the Victim and Who is the Fraudster? Reviewing the Procedural Position of the Victim in Fake President Fraud Cases, and How to Reframe it?

Gábor Damjanovic and Réka Bali

Abstract

In recent years, “fake president fraud” cases have become particularly widespread. In this article, Gábor Damjanovic and Réka Bali of Forgó Damjanovic and Partners, Budapest explore the phenomenon of fake president fraud cases and examine the Hungarian legislative framework and the practice of conducting criminal procedures in such cases.

1. What Constitutes “Fake president fraud”?

“Fake president fraud” is a term that is purposefully not in line with the precise terminology of Hungarian criminal law. The phenomenon is closest to Section 373 of the Hungarian Penal Code which defines “fraud” in the following way:

“when a person uses deceit, deception, or trickery for unlawful financial gain, and thereby causes damage”.

By using the term “fake president fraud”, we refer to cases where perpetrators deceive victims by presenting themselves as the agent of the victim’s contractual partner. They forge email addresses (“Business Email Compromise”) and invoices in order to indicate that the bank account of the creditor has changed. They ask the debtor to carry out future payments to their new bank account. The bank accounts used to receive these payments are usually ones pertaining to companies founded with the use of forged identification documents and typically established just a few days before the actual fraud takes place and typically for the single purpose of the fraud. One of the peculiarities of this type of fraud is that the payment is almost

immediately forwarded to another foreign bank account and keeps on being forwarded to other ones, acting as “Money Mules”.

This type of fraud has become more and more frequent in the last couple of years. The amounts of money acquired in this manner have increased noticeably and typically range from EUR 200k to 3M. The fact that Hungarian bank accounts are used particularly often in these fraudulent actions makes it especially relevant to study the procedural norms in the Hungarian legislative framework, as well as the related practice.

2. Hungarian Practice and Jurisdiction Issues

2.1. The Status of the Wronged Party

Hungarian authorities typically do not deem the wronged party to be a victim in the course of criminal proceedings. The reasoning behind this practice is partly due to the question of qualification of the crime and also connected to jurisdictional issues.

In cases where the wronged party - typically a foreign corporation - wishes to participate in the proceedings, Hungarian authorities only allow them to do so under the status of a “*party with pecuniary interests*”. The definition of a “*party with pecuniary interests*” is as follows:

“Party with pecuniary interests means a natural person or a legal entity that is:

- a) the owner of or holds any ownership rights over a confiscated or seized thing,*
- b) entitled to dispose of any asset that may be subject to forfeiture, or*
- c) entitled to dispose of any electronic data that may be rendered to be permanently inaccessible.”¹*

In fake president fraud cases, the wronged party qualifies as a party with pecuniary interests because its assets - the money which the fraudster acquired - are subject to seizure and forfeiture.

Under Hungarian law, this status limits the options of the person concerned, since it only grants certain procedural rights: fewer ones than those of a victim. Among others, the party with pecuniary interests has the right to

“a) submit evidence, file motions and observations concerning matters affecting him/her,

¹ Section 57 (1) a)-c) of Act XC of 2017 on criminal proceedings

- b) be present at procedural acts directly affecting the thing, asset, or electronic data subject to his/her right of disposal,*
- c) become familiar with the ground and its changes of a coercive measure affecting the thing, asset, or electronic data,*
- d) receive information of his/her rights and obligations in the proceeding from the court, prosecutor office, or investigating authority,*
- e) seek legal remedy concerning matters affecting him/her,*
- f) have access to the case's documents concerning matters affecting him/her,*
- g) use an aide.”²*

However, even the abovementioned rights can be restricted:

“Notification of the party with pecuniary interests may be omitted, and/or a party with pecuniary interests may be removed from the site of a procedural act, if doing so is necessary due to the nature or urgency of the procedural act, or for guaranteeing the safety of another person involved in the criminal proceeding.”³

In comparison, victims are entitled to

- “a) submit evidence, file motions and observations,*
- b) speak in the course of closing speeches,*
- c) be present at hearings and other procedural acts and raise questions,*
- d) become familiar with the case's documents,*
- e) receive information of his/her rights and obligations in the proceeding from a court, prosecutor office, or investigating authority,*
- f) seek legal remedy,*
- g) use an aide,*
- h) enforce a civil claim in the court procedure as a civil party, and declare his/her intent to do so during the investigation,*
- i) act as a private prosecutor or a substitute private prosecutor.”⁴*

Therefore, wronged parties trying to help the proceedings by joining in do not have the option to fully participate and get all necessary information to trace their lost funds properly. This is highly controversial as they are without doubt the victims of a fraud. Therefore, Hungarian authorities only commence proceedings on suspicion of money-laundering, and do not consider fraud or falsification of documents as a cause of action. Since money-laundering is a crime committed against the overall financial interests of a state, this approach does not permit the authorities to view the wronged party as a victim. As a result, it is difficult to get information about the transferred funds, their status and location. As such, the wronged party cannot

² Section 57 (2) a-g) of Act XC of 2017 on criminal proceedings

³ Section 57 (3) a-b) of Act XC of 2017 on criminal proceedings

⁴ Section 51 (1) a-i) of Act XC of 2017 on criminal proceedings

immediately turn to the next money mule station for help and/or the freezing of the funds.

We note that although the party with pecuniary interests also has the right to information, this is only a limited right to information. We find that the authorities interpret this restrictively and do not provide the most necessary information, including details of further transfers.

2.2 Jurisdiction of Hungarian Authorities and Courts

As mentioned above, the reasoning behind this practice is mostly connected to jurisdictional issues. Authorities typically assume that there are foreign victims of the crime; therefore, they consider the crime to have been committed abroad. However, a number of professionals suggest that - in cases of fraud - there are other factors that could serve as grounds for jurisdiction.

If one considers the territorial and personal scope of the Hungarian Penal Code, one can establish that Hungarian authorities have jurisdiction not only if the victim is Hungarian, but also, inter alia, if the criminal offences are committed in Hungary or by a Hungarian national abroad if the act constitutes a criminal offence under Hungarian law. In case of fake president fraud, deceiving someone takes a complex course of action - several stages of which may take place in Hungary. (Fake) Hungarian companies, invoices, bank accounts, managing directors and banking institutions are all factors that tie the case to Hungary and therefore could serve as grounds for jurisdiction.

We believe that this approach is also supported by legal literature on the Hungarian Penal Code. According to Krisztina Karsai, in the commentary of the Hungarian Penal Code:

“An act shall be deemed committed in Hungary even if there are elements of the act that have been realised abroad: the unit theory of action is also applicable for the application of this provision, so the act is deemed committed in Hungary if any (objective) element of the crime is realised in Hungary. [...] With regard to acts committed abroad by a Hungarian citizen, the active person principle underlying the application of the Hungarian Penal Code applies without restriction: a Hungarian citizen is liable for an offence committed abroad.”(emphasis added).⁵

Thus, if even one element of the crime is related to Hungary, or there is a suspicion that the perpetrator is Hungarian, Hungarian jurisdiction may already be well-founded, which creates an opportunity to initiate criminal proceedings for fraud.

⁵ Karsai Krisztina - Commentary on Act C of 2012 on the Penal Code

3. Conclusion

In view of the above analysis, we consider that the practice of the Hungarian investigative authorities to not initiate an investigation into a foreign victim due to a fraudulent act prevents the victim from taking the necessary measures to recover the damage caused through fake president fraud. If the victim makes the report abroad, the foreign authorities must also contact the Hungarian bank holding the relevant account through the Hungarian authorities, thus increasing the time required to obtain vital information.

We are of the opinion that there is no need to amend the Hungarian Penal Code or the procedural rules, but the Hungarian investigative authorities shall apply the tools they already have to help the victims of fake president fraud cases. On the one hand, this could be solved by launching an investigation for fraud where the wronged party qualifies as victim. On the other hand, it is also helpful if the wronged party's right to information as a party with pecuniary interests is interpreted more broadly by the authorities, and they provide the wronged party with the information needed to find the funds transferred abroad.

What shall be reframed are not the applicable laws but the approach of the Hungarian investigative authorities. A number of professionals dealing with fake president fraud cases - including one of the authors of this article - have recently turned to the criminal Deputy Attorney General to request a change of the practice in accordance with the above. The initial answer from the criminal Deputy Attorney General was positive; nevertheless, whether the above practice will actually change is yet to be seen.

About the Authors

Gábor Damjanovic is co-managing partner of Forgó Damjanovic & Partners Law Firm. He heads the Dispute Resolution Practice Group and handles complex, high-value commercial court cases and arbitrations, as well as fraud cases; almost always with a cross-border element. Gábor is frequently nominated as an arbitrator, both as wing and chair and has represented clients/acted as arbitrator under a number of different institutional rules, as well as under the UNCITRAL rules. According to Legal 500: “*Gábor Damjanovic stands out for his ‘impressive practical knowledge in court cases and arbitration’*”. Gábor is also listed on the Arbitration Powerlist 2021 CEE published by the Legal 500.



Contact Gábor Damjanovic: T. +36 30 280 7839; E. damjanovicg@fdlaw.hu



Réka Bali is an attorney-at-law at Forgó, Damjanovic and Partners Law Firm. She is specialised in litigation and commercial law. She works on several complex litigation cases which require comprehensive approach and deep understanding both of law and practice in the area of commercial relations. She has extensive experience in fake president fraud cases.

Contact Réka Bali: M: +36 30 199 9426; Email: balir@fdlaw.hu

Beneficial Ownership: An Overview of the Senegalese Institutional Framework

Dr Aboubacar Fall

Abstract

In this paper, Dr Aboubacar Fall, Senior Partner of AF Legal Law Firm, provides the readers with an overview of the new Senegalese legal and institutional framework which aims at bringing transparency in the business field while achieving other objectives such as preventing fraud, fighting money laundering as well the financing of terrorism. One of the main feature of the beneficial owners' legislation and regulation is reflected in the creation of a national Registry. Indeed, this legal body is tasked with the mission of scrutinizing the company's ownership and, if necessary, imposing judicial as well as financial sanctions. Senegal is one of the rare African countries to address the beneficial ownership as a main governance and doing business related issue.

Introduction

As a member of the Extractive Industries Transparency Initiative ('EITI'), Senegal is compelled to implement the EITI Norm in incorporating a beneficial ownership information framework. Another requirement calls for the establishment of a public register designed to identify owners who benefit from investment contracts in the extractive sector - including, but not limited to, mining, oil and gas. In fact, it has not been difficult for the government of Senegal ('GoS') to comply with this mandate due to the existence of a favourable regional and domestic legal environment. Indeed, the West African Economic & Monetary Union ('WAEMU') Directive N°02/2015 of 2 July 2015 on the fight against Money Laundering and Terrorist Financing already provides for the definition of the concept of 'beneficial owner'. At the national level, Law No. 3/2018 dated 23 February 2018 relating to the fight against money laundering and terrorist financing was adopted by the National Assembly on 13 February 2018.

It is worth noting that the implementation of mandatory disclosure of beneficial ownership is an integral part of the global fight against corruption, conflicts of interest, tax evasion, money laundering and illicit financial flows, which has increased since the "Panama papers" scandals. The term *beneficial owner* is often referred to as "*beneficial ownership*", or "*economic beneficiary*", but today, the term *beneficial owner* is preferred and used both in the framework of the reforms of the extractive industries sector as well as in the international tax sector.

Who are the Beneficial Owners?

The following have been designated and identified by Senegalese law as beneficial owners:

- Natural persons who own or control, directly or indirectly, the registered legal or natural person or declaring activity;
- Individuals who directly or indirectly hold at least 2% of the capital and voting rights of the reporting company;
- Natural persons who exercise, by other means, a power of control over the management, administrative or executive bodies of the reporting company;
- In the absence of identification according to the two preceding criteria, the beneficial owners are the natural persons who directly or indirectly occupy the position of legal representative of the reporting company, in particular through one or more legal persons.

What are the Different Forms of Ownership?

The different forms of ownership are divided into (i) legal ownership and (ii) beneficial ownership.

These concepts are explained as follows:

1 - *Legal ownership*: means any person holding the legal title of a movable or immovable property. This legal owner can be a natural or legal person. It is called apparent ownership.

2 - *Beneficial owner*: means any hidden, concealed, undisclosed person who controls the person whose identity is revealed. There is a barrier or an overlap of apparent owners. Under the Financial Action Task Force framework, the beneficial owner must be a natural person.

The Regional Legal Framework

The notion of beneficial owners finds its basis in regional legal instruments such as:

- Compliance with the requirements of the EITI since 1 January 2020 on the transparency of beneficial owners (Requirement 2.5);
- Compliance with community commitments derived from Directive n°2/15/CMUMOA of 2 July 2015 on the Fight against Money Laundering and Terrorist Financing, transposed into national legislation by Law of 23 February 2018;
- Regulation n°08/2008/CM/UEMOA of 26 December 2008 adopting rules for the avoidance of double taxation and rules of assistance in tax matters;
- Article 13.4 of the Economic Community of West African States ('ECOWAS') Mining Directive C/DIR of 27 May 2009;
- Meeting the objectives of transparency and legal certainty pursued by OHADA law (Article 35§3 of the Uniform Act on Commercial Law);
- Compliance with the standards of exchange of information for tax purposes by signing the OECD Multilateral Convention on Mutual Administrative Assistance; the Convention on the Implementation of Measures Relating to Tax Treaties to Prevent the Erosion of the Tax Base and the Transfer of Profits.

The National Legal Framework

This is enshrined in the following legal instruments:

- Art. 25-1 of the Constitution;
- Law n°2008-12 of 25 January 2008 on the protection of personal data;
- Art. 1 of Law 2018-03 of 23 February 2018 on AML/CFT;
- Art. 55 of Law 2019-03 of 1 February 2019 on the Petroleum Code; arts. 10 and 16 of Decree no. 2020-2061 of 27 October on the application of the Petroleum Code; art. 18.1 of the model CRPP
- Art. 3 of decree n°2020-2065 fixing the modalities of participation of Senegalese investors in oil companies of 28 October 2020;

- Art. 95 and 96 of Law n° 2016-32 of 8 November 2016 on the Mining Code;
- Art. 14 of law n° 2020-06 of 7 February 2020 on the Gas Code;
- Art 17 and 18 of law n° 2012-31 of 31 December 2012, as amended, on the General Tax Code;
- Decree n° 2020-791 of 19 March 2020 relating to the Register of Beneficial Owners and Ministerial Order n° 1598 of 5 February 2021 relating to the form of the declaration govern the modalities of implementation of beneficial ownership
- Article 56 of the LFR adopted on 3 June 2021 modifying article 633 of the CGI extends the obligation of declaration.

The main risks associated with hidden properties are well documented. These include the lack of transparency and discretion in tendering processes; undisclosed or incorrect ownership data; owners who are politically exposed persons ('PEPs'); shareholding structures involving companies incorporated in so-called 'tax havens' or low-tax countries; and, that shares are divided in such a way that each owner holds fewer shares than the reporting threshold.

Beneficial Ownership Disclosure Related Issues

Several issues can be identified with the disclosure of beneficial owners at the national level. For governments, it is a national security issue. Knowing the identity of those operating in the sector guarantees ownership of resources to the people. Further, it is a matter of oversight in holding accountable those behind companies. It is also a revenue mobilization issue. For companies, it promotes healthy competition and due diligence as well as the knowledge of the identity of all business partners. For civil society, the issue of transparency and accountability provides the possibility to demand accountability and scrutinise. Lack of beneficial ownership information creates several issues such as complex capital trails that are difficult to trace as well as chains of shell companies and layers of experts or legal arrangements. Only transparency of beneficial owner will ensure that those pulling the strings, their associates and facilitators will stop operating in secrecy.

The Extractive Industries Transparency Initiative ('EITI') in Senegal

The EITI is a global initiative launched in 2002 to promote better governance in resource-rich countries. The EITI Standard requires the publication of information

on the entire value chain of extractive industries, from the point of extraction of natural resources to how revenues are collected by the government and how they are used to benefit people. At the international level, oversight of the Initiative is provided by a Board of Directors led by a Chairperson and composed of representatives from implementing countries, donors, partner countries, international and national oil, gas and mining companies, and civil society. Supported by a Secretariat, the International EITI Board ensures that the requirements of the EITI Standard are met.

Senegal joined the EITI in October 2013, when it was declared a "candidate country"- actually equivalent to an "implementing country". The EITI is implemented by a National Committee established by Decree 2013-881 of 20 June 2013. The National Committee is chaired by a Minister attached to the Presidency of the Republic, and includes twelve (12) representatives of the Administration, six (6) representatives of extractive companies, six (6) representatives of Civil Society (Order of Chartered Accountants and the Press included), two (2) representatives of the National Assembly and one (1) representative of local elected officials. The National Committee is supported by a Technical Secretariat. Since its accession, the country has undertaken the implementation of the Standard through activities aimed at strengthening transparency in the management of revenues from the extractive sector. These activities are defined in the annual work programs approved by the Multi-Stakeholder Group (the National EITI Committee - CN-ITIE). The Committee adopted in 2017 a strategic plan covering the period 2017-2021¹⁵. The working documents are available on the Committee's website.¹

The EITI's Normative Expectations for Beneficial Ownership Disclosure

- The EITI, as a Global Standard, requires that from 1 January 2020 implementing countries require companies to disclose beneficial ownership information (Requirement 2.5)
- The scope of this requirement includes:
 - Companies that are in the process of acquiring or holding interests in the extractive sector
 - The country must allow disclosure of beneficial ownership, the degree of ownership, and certain information about how ownership is held or control is exercised

¹ See : www.itie.sn (accessed 30 September 2021).

- For the EITI, the legal framework in force must allow for the identification of the following points
 - Competent authority
 - Definition of beneficial owner
 - Reporting entities
 - Beneficial owner information
 - Verification of data
 - Penalties for misrepresentation or non-disclosure
 - Public Access.

Decree on the Registrar of Beneficial Owners ('RBE')

Decree n°2020-791 has five chapters and sixteen articles. It deals with the following : creation of the Register of Beneficial Owners (RBO) , procedure for the declaration of beneficial owners, identification of beneficial owners, access to the information of beneficial owners, sanctions in case of false declaration or non-disclosure.

Creation of the RBE at the Registry in Charge of the National Company Registration System ('RCCM')

The BRE is under the supervision of the judge in charge of the RCCM (French acronym of the National Company Registration System). Registration is carried out in electronic format and the protection of personal data is guaranteed and respected. The register mentions the chronological order of filing, the date and the serial number of the declarations relating to the Beneficial Owner (BO) Each declaring entity has an individual file. The mandatory Reporting entities are the following: commercial companies, sole proprietorships, contractors and other entities registered or declared in Senegal involved in the value chain of the extractive sector, as well as companies operating and not registered in Senegal (Cf. art. 1, 2 and 3 of decree n°2020-791).

Other African countries which have set up beneficial ownership registers include Nigeria, Ghana & Zambia.

Declaration of Beneficial Owners

The declaration should be dated and signed by the legal representative of the company or the legal entity making the declaration. This is made on the basis of a form established by order of the Ministry of Justice. Art 4 of the decree related the information on the declaration form which are the following :

- identity of the registered entity; full name(s), nationality(ies), country of residence, national identification number(s), date of birth, home and residence addresses of beneficial owners; date of acquisition of beneficial ownership;
- Identify any PEP with the following information: First and last names, date of birth, nationality, countries of residence, date of acquisition of ownership, service address; First and last names of the office holder, date of commencement of office, date of termination of office; Nature of the relationship between the PEP beneficial owner and the office holder.

The Central Roles of the Registrar (Articles 5 & 6)

Articles 5 & 6 of the decree set out the different roles the Registrar has to perform.

These will consist of the following:

- Present the form to the applicant;
- Inform about the existence of administrative sanctions in case of failure to declare;
- Possibility for the applicant to file, together with the other documents related to the registration or 15 days after the registration;
- Occasionally presents the form for any modification or complementary registration or in case of deletion.
- Possibility to refer to the judge assigned to the supervision of the RBE by the clerk, in case of refusal of declaration by the applicant, to order the latter to proceed to the declaration under penalty.
- The clerk verifies the accuracy of the declaration; in case of inaccurate declaration, informs the judge and the prosecutor.

- In the absence of a response from the judge assigned to supervise the Registry within 10 days of the referral by the clerk, the latter completes the formality in the terms formulated by the applicant (art. 8 of the decree).

The intervention of the judge in charge of the register is to rule by way of an Order, either at the request of the Public Prosecutor's Office or the Clerk of the Court in charge of the RBO to enjoin any entity subject to the declaration to comply. In case of non-execution, the judge will note the failure to comply on the basis of the report drawn up by the clerk of the court. The entity can exercise its right of appeal against the judge's Order (as per Art. 7 of the decree).

Access to the Registry of Beneficial Owners

It is important to note that the decree has set two (2) forms of access: one, which is free, is for the public authorities and the other, which is conditional, is designed for natural and legal persons.

1- Free access of the public authorities (art. 12)

- The declarations relating to the BOs are transmitted without delay or financial consideration, at their request, to the following authorities :
- Magistrates and judicial police officers within the scope of their duties;
- The Director General of Public Accounts and the Treasury;
- The Director General in charge of the Budget;
- The Director in charge of Mines;
- The Director in charge of hydrocarbons;
- The Director General of Customs;
- The Director General of Taxes and Domains;
- The President of the EITI;
- The President of the body in charge of the fight against fraud;
- The President of the body in charge of processing financial information;
- Any other authority designated by law;

2- Conditional access for natural and legal persons:

This information is only accessible to natural and legal persons who make a request to the judge in charge of the supervision of the RBO, and who justify a legitimate interest. These persons have the right to lodge an appeal in case of refusal by the judge.

Conclusion

In line with international best practices, Senegal has enacted a new legislation with the overarching objectives of:

- (i) Attracting foreign investments of good quality,
- (ii) Creating a favourable business environment for all companies operating in the country,
- (iii) Fighting corruption, tax evasion, money laundering and terrorism financing,
- (iv) Preventing the risk of conflict of interest,
- (v) Avoiding illicit financing flows, and
- (vi) Increasing the State revenue

To that end, the government has put in place legal and institutional tools, such as the Registry, designed to achieve a great transparency in doing business and prevent commercial fraud. In that regard, it is worth mentioning that Senegal is among the first African countries to be equipped with such a legal framework which, it is hoped, will prove to be highly productive for business and investment.

About the Author



Dr. Aboubacar Fall is Senior Partner at AF Legal, Dakar, Senegal. He is a member of the Senegal Bar and a former member of the Paris Bar (France). He holds a PhD in International Business Law from University of Rouen -Haute Normandy (France) a Masters (LL.M) from University of Washington in Seattle (USA), a Masters in International Transportation from University of Paris 1- Pantheon-Sorbonne (France) and two Certificates in Petroleum Policy & Management from PETRAD Foundation in Stavanger (Norway).

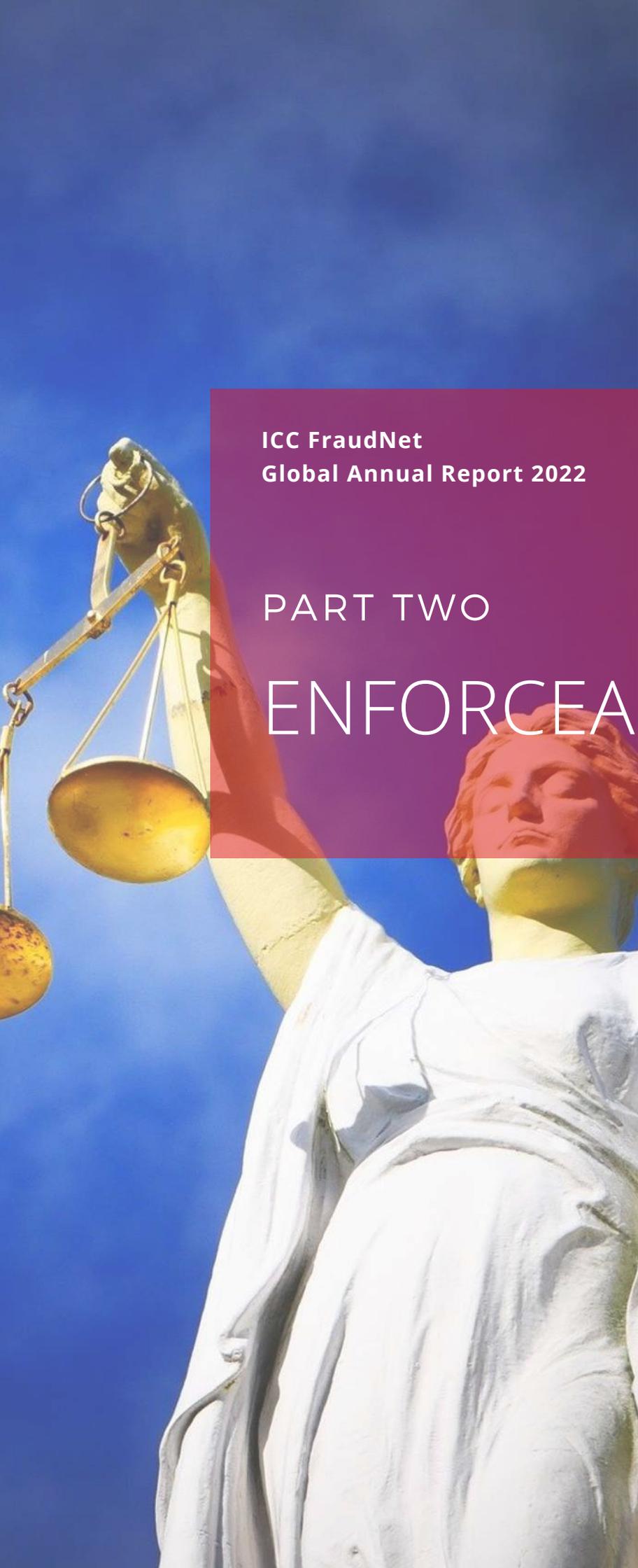
He has been practicing law for over 30 years, and worked for over 10 years as Principal Legal Counsel for the African Development Bank (AfDB) Group and has served for 3 years as Chairman of the Management Board of the African Legal Support Facility. From January 2015 to October 2018, he was a partner at Geni & Kebe law firm in Dakar. In 2015 & 2016, he was nominated as one of the 100 most influential people in Africa by the magazine Financial Afrik.

In 2018, he was nominated by Financial Afrik among the 18 most active law firms' leaders in Africa. Dr. Fall's areas of expertise include, among others, banking & finance, maritime & aviation, international business, trade finance, project finance, private equity and M&A , energy, mining, oil & gas, infrastructure (PPP), fraud & white-collar crime, international (commercial & investment) arbitration, & ADR.

He is a member of several professional organizations including the Association of International Petroleum Negotiators, International Energy Law Advisory Group, International Bar Association, the Union Internationale des Avocats, ICC FraudNet, African Arbitration Association, Comité Maritime International (CMI), African Arbitration Association, the London Court of Arbitration. In 2017 & 2018, he was nominated in the Who's Who Legal as Asset Recovery Expert.

Dr Fall holds several teaching positions in Senegal and abroad including the UN Institute for Training & Research in Geneva, and the Institut Supérieur de Droit de Dakar, and the Institut des Métiers du Droit. He is currently the Program Director of the Center for International Law Practice, and has been appointed in 2019 as a member of the Board of Directors of the International Lawyers for Africa (ILFA) Program.

Contact Dr Fall: T. +221338250300; E. a.fall@aflegal.sn



ICC FraudNet
Global Annual Report 2022

PART TWO

ENFORCEABILITY

The Extraterritorial Application of Asset Forfeiture Proceedings in South Africa

Michael-James Currie, John Oxenham and
Jemma Muller

Abstract

In this article, Michael-James Currie, John Oxenham and Jemma Muller, of Primerio International, South Africa analyse recent case law which has significantly developed South Africa's efforts in international asset recovery, particularly in the fight against corruption. The authors provide an overview of the impediments to effective international asset recovery efforts in South Africa, with a particular focus on issues regarding extraterritorial jurisdiction and international cooperation.

Introduction

The large-scale corruption which made up 'State Capture' has plagued South Africa and has resulted in billions of Rands being illicitly diverted abroad. As a result, there is now a renewed vigor by the public and private sector in seeking to repatriate monies and assets which were the subject of corrupt activities. For a variety of reasons, which we discuss more fully below, the South African National Prosecuting Authority ('NPA') has had limited success in successfully identifying and repatriating ill-gotten gains to South Africa.

Since President Cyril Ramaphosa was elected in February 2018, South Africa's Government has taken significant steps to a) root out corruption through the establishment of various judicial commissions of inquiry and b) rebuild the institutions required to prosecute corruption and recover the proceeds of such crimes.

The most notable of these have been the establishment of the Judicial Commission of Inquiry into Allegations of State Capture, Corruption and Fraud in the Public Sector including Organs of State ('Zondo Commission') in August 2018. This is set to

conclude on 31 December 2021.¹ The latest development to the Regulations of the Zondo Commission², (although in reality a public institution), highlight the potential benefits of collaboration between enforcement agencies and private bodies. In this regard, the Zondo Commission is an independent body, employing a number of private sector individuals who now, in terms of the Regulations, are permitted to not only share evidence, but to also consult directly to the enforcement agencies.

Despite having unearthed a commendable amount of information surrounding the amount and manner in which funds have been diverted abroad³, the Zondo Commission has cost South African taxpayers approximately ZAR 1 billion to date (approximately USD 67,204,300⁴).⁵ Of equal concern is that public enforcement and recovery efforts will be delayed significantly.

In addition to the establishment of the Zondo Commission, the Special Investigating Unit's ('SIU') Special Tribunal was established in February 2019. The SIU Special Tribunal is expressly tasked with fast-tracking the recovery of assets stolen from Government and various state-owned entities.⁶ Despite the initial positive reception regarding the potential benefits of the SIU Special Tribunal, recent statistics have shown that asset recovery cases have fallen short of expected targets. The National Prosecuting Authority's Annual Report ('NPA Annual Report') states that for the 2019/2020 financial period, a mere ZAR 200 000 (approximately USD 13,441⁷) recoveries were made in relation to government-related corruption. Evaluated against a ZAR 600 million target (approximately USD 40,322,580⁸), the efficacy of the SIU in repatriating funds from abroad is questionable.⁹

Where the recovery of assets required cross-border tracing and recovery of assets out of South Africa, the amounts are significantly lower. This is despite the fact that

¹ *Chairperson of the Judicial Commission of Inquiry into Allegations of State Capture, Corruption and Fraud in the Public Sector including Organs of State v President of the Republic of South Africa and Others* 46878/21.

² Regulations of the Commission on State Capture, Corruption and Fraud in the Public Sector including Organs of State, < https://www.statecapture.org.za/uploads/r24_of_2020.pdf > accessed 9 June 2021.

³ Paul Holden, "Part Three: The local and international laundries used by the Gupta enterprise and its associates" (29 June 2021) <https://www.dailymaverick.co.za/article/2021-06-29-part-three-the-local-and-international-laundries-used-by-the-gupta-enterprise-and-its-associates/> > accessed 8 July 2021.

⁴ ZAR 1 billion converted at ZAR/USD rate of 1 : 0.067.

⁵ "State Capture Inquiry Raymond Zondo briefs the media on commission's work during to date" (30 June 2021) < <https://www.statecapture.org.za/site/media/briefings> > accessed 8 July 2021.

⁶ "President Cyril Ramaphosa appoints Special Investigations Tribunal" (24 February 2019) < <https://www.gov.za/speeches/president-ramaphosa-appoints-special-investigations-unit-tribunal-24-feb-2019-0000> > accessed 10 June 2021.

⁷ ZAR 1 billion converted at ZAR/USD rate of 1 : 0.067.

⁸ ZAR 1 billion converted at ZAR/USD rate of 1 : 0.067.

⁹ National Prosecuting Authority Annual Report for the 2019/2020 financial period, 128.

South Africa has a modern legislative framework in place to assist in prosecuting corruption and recovering assets offshore.

Critique regarding South Africa's enforcement activities has largely centered around issues such as capacity constraints and skill shortages at key investigative and prosecutorial agencies. While efforts have been made to address these concerns, the lack of proper enforcement over the last decade or two, since the enactment of South Africa's new corruption and asset recovery laws, has caused a lack of clear legal precedent on the interpretation of these laws, particularly on issues of extraterritorial jurisdiction and international cooperation.

We have in this article provided an update on recent case law which now provides insight in relation to the extraterritorial application of South Africa's corruption and asset recovery laws. These case developments are certainly welcomed as they will have far-reaching ramifications for extraterritorial application of asset forfeiture proceedings in South Africa.

Extraterritorial jurisdiction

The doctrine of effectiveness, in the context of the international law on jurisdiction, has often been raised as a key impediment to international asset recovery. In terms of this doctrine, a court should only assert jurisdiction in matters where it is able to give effect to its order. In other words, a court would not exercise jurisdiction over a matter where, it appears, that the order will ultimately be ineffective in that it cannot be enforced against the defendant (as the defendant has no assets in the jurisdiction of the court).

Recent South African case law confirms that the common law position in South Africa is of equal application, unless there is any legislative provision which specifically excludes the doctrine.

In this regard, the primary legislation dealing with the recovery of proceeds of unlawful activity is the Prevention of Organised Crime Act, 121 of 1998 ('POCA'). The relevant enforcement agency in this respect is the Asset Forfeiture Unit ('AFU'), a division of the NPA which is headed by the National Director of Public Prosecutions ('NDPP'). Asset forfeiture under POCA can take place either under Chapter 5 ('criminal forfeiture') or under Chapter 6 ('civil forfeiture').

In terms of criminal forfeiture, and as provided for in section 18(1) of POCA, the restraint and/or confiscation and, where applicable, the realisation of the value of

benefits derived by virtue of a crime that may be realized, is dependent on the accused first being convicted of an offence.

The restriction does not apply to civil forfeiture, wherein the preservation and forfeiture of property specifically deals with property that is believed to be the proceeds of unlawful activities or which is an instrumentality of an offence referred to in Schedule 1 of POCA.¹⁰ Notwithstanding this, the AFU must still show criminality under civil forfeiture and preservation applications instituted under sections 38 and 48 of POCA. Naturally, criminal forfeiture proceedings take longer to launch than civil forfeiture proceedings due to the inherent delays in securing the conviction of the accused in criminal proceedings, which has a direct bearing on the ability of the AFU to obtain a confiscation order and hence the AFU's adoption of the initiative to rather focus on civil forfeiture proceedings.¹¹

As discussed below, the deviation from the common law doctrine of effectiveness is expressly provided for by section 19(1) of the International Co-operation in Criminal Matters Act, 75 of 1996 ('ICMM Act') in terms of which a court may request foreign authorities to assist in the enforcement of a court's confiscation order in circumstances where it can be established that the person against whom the order was granted has property in that foreign jurisdiction. Evidently, section 19(1) aims to provide South African Courts with the appropriate mechanism to enforce its judgments, specifically confiscation orders, where property is located within a foreign jurisdiction.

The *Bobroff I* Case

The practical implementation and interpretation of POCA in the context of forfeiture of proceeds of unlawful activities located in a foreign state was considered at length in the case of *The National Director of Public Prosecutions v Darren Rodney Bobroff and Ronald Bobroff*¹² ('Bobroff I').

In *Bobroff I*, an application for a civil forfeiture order was made by the State, under section 48 of POCA, seeking the forfeiture of the credit balances and interest accrued in two bank accounts which were held by the respondents in Israel. The State argued that the proceeds were fraudulently obtained in contravention of the Contingency Fee Act, 66 of 1997.

¹⁰ Prevention of Organised Crime Act 1998 ("POCA"), s 38(2). See also Schedule 1.

¹¹ National Prosecuting Authority Annual Report for the 2019/2020 financial period, 124 which contains the following statement "Delays in the finalization of criminal investigations and the drafting of charge sheets have had a significant impact on the AFU's ability to meet its performance targets".

¹² *The National Director of Public Prosecutions v Bobroff and another* [2019] JOL 45485 (GP) ("*Bobroff I*").

The State had successfully applied for and obtained a preservation order against the respondents on the basis that the funds were deemed to have been proceeds of unlawful activities¹³. In the application for the forfeiture of the assets, the applicant (being the NDPP) had to prove, on a balance of probabilities, that the property concerned (i.e. the bank balances and accrued interest) constituted “*proceeds of unlawful activities*”.¹⁴

The respondents in *Bobroff I* contested the High Court’s jurisdiction in respect of an application for the civil forfeiture of the credit balances and interest accrued on two bank accounts held in Israel.

Therefore, the crux of the case turned on whether South African Courts had jurisdiction to forfeit property located outside of South Africa. The respondents argued that, since the bank accounts are located in Israel, it falls outside the territorial jurisdiction of the High Court because the court has “*no jurisdiction in respect of the property situated outside the borders of the Republic, even if the defendant is an Incola of that court*”.¹⁵

The High Court in *Bobroff I* confirmed that the territorial jurisdiction of South African Courts is subject to specific legislative provisions that provides our courts with extraterritorial jurisdiction.¹⁶ Accordingly, the question that had to be determined by the High Court was whether “*there [was] any empowering legislation that gives jurisdiction in respect of proceedings against property that is beyond [South Africa’s] borders in terms of POCA.*”¹⁷

The High Court found that the definition of “*proceeds of unlawful activities*” contained in POCA¹⁸ provided the High Court with jurisdiction over property that is

¹³ As contemplated in section 38(2)(b) of POCA

¹⁴ POCA, s1(1)(xv) defines “proceeds of unlawful activities” as “*any property or any service, advantage, benefit or reward which was derived, received or retained, directly or indirectly, in the Republic or elsewhere, at any time before or after the commencement of this Act, in connection with or as a result of any unlawful activity carried on by any person, and includes any property representing property so derived*”.

¹⁵ *Bobroff I*, [21].

¹⁶ *Bobroff I*, [33].

¹⁷ *Bobroff I*, [22].

¹⁸ POCA, s1(1)(xv). Furthermore, the High Court also referred to the Preamble to POCA which states: “*AND WHEREAS no person should benefit from the fruits of unlawful activities, nor is any person entitled to use property for the commission of an offence, whether such activities or offence took place before or after the commencement of this Act, legislation is necessary to provide for a civil remedy for the preservation and seizure, and forfeiture of property which is derived from unlawful activities or is concerned in the commission or suspected commission of an offence*”, read with the amended section 1 definition of “confiscation order” contained in section 1 of the ICMM Act, which has been amended to include “a forfeiture order made under the Prevention of Organised Crime Act, 1998”. See also the introduction of the Act which states that its purpose is to, *inter alia*, facilitate the confiscation and transfer of the proceeds of crime between the Republic and foreign States.

situated abroad and in respect of which a forfeiture to the State order has been made, provided it constitutes the proceeds of unlawful activities.

Accordingly, where assets are sought to be forfeited by means of civil proceedings, the *Bobroff I* case confirms that, where those assets constitute “*proceeds of unlawful activity*”, the mere fact that the assets are no longer situated within the territory of South Africa does not preclude South African Courts from exercising jurisdiction in respect of those assets.

Although the *Bobroff I* decision did not expressly provide for the above-mentioned principle in relation to “criminal forfeiture” matters, the principle would presumably be of equal application in instances of criminal forfeiture matters. This is due to the fact that the definition of a “confiscation order” within the ICMM Act does not distinguish between criminal and civil forfeiture orders and the definition of “instrumentality of an offence” in POCA does not preclude property used in the committal of a criminal offence outside of the Republic.¹⁹

Bobroff II²⁰

The *Bobroff I* decision was taken on appeal to the Supreme Court of Appeal (‘SCA’), with judgment recently handed down on 3 May 2021.

Bobroff’s appeal was based on two grounds, namely: (i) whether the High Court had jurisdiction to make a forfeiture order in terms of section 50(1)(b) of POCA; and (ii) whether the NDPP had established that the forfeited property were “proceeds of unlawful activities”, as defined in POCA.

The SCA upheld the decision of the High Court. With regards to jurisdiction, the SCA expanded the High Court’s interpretation and found that section 19 of the ICMM Act specifically provides for a mechanism of enforcement of foreign forfeiture orders. Section 19(1) states:

“When a court in the Republic makes a confiscation order, such court may on application to it issue a letter of request in which assistance in enforcing such order in a foreign State is sought if it appears to the court that a sufficient amount to satisfy the order cannot be realized in the Republic and

¹⁹This is by virtue of consideration of section 1 of the ICCM Act as well as the definition of instrumentality of an offence” contained in POCA, which is defined as:

“any property which is concerned in the commission or suspected commission of an offence at any time before or after the commencement of this Act, whether committed within the Republic or elsewhere.” (our emphasis)

²⁰ *Bobroff and Another v The National Director of Public Prosecutions* (Case no 194/20) [2021] ZASCA 56 (3 May 2021) (“*Bobroff II*”).

that the person against whom the order has been made owns property in the foreign State concerned.”

Request for Mutual Legal Assistance (‘MLA’)

As mentioned in the *Bobroff II* judgment²¹, section 19 of the ICMM Act makes provision for a court in South Africa that has made a confiscation order to request assistance from a foreign State for enforcement of an order.

While use of MLA is key to the application of extra-territorial jurisdiction, MLA has only been used by South Africa in a very limited number of cases.

In the 2019/2020 year, however, the NPA received 86 requests for MLA from foreign states and 6 requests were initiated by South Africa and transmitted to the relevant foreign states.²² Of these requests for MLA, a total of 42 requests were finalized.²³ Of the total requests for MLA, 18 were initiated by South Africa.²⁴

According to the NPA Annual Report, outgoing MLA requests are “*highly challenging in nature due to the complexities and delays involved in the execution and/or processing of such MLA [...] requests.*”²⁵ In emphasizing these challenges, the head of the NPA, Shamila Batohi, stated that extradition involves prolonged legal proceedings and that there is also a political aspect in that the executive must decide whether or not to surrender a person to the requesting country.²⁶ Moreover, South Africa has, generally, entered into very few extradition agreements.

As at the beginning of 2021, South Africa only has extradition treaties with 14 other countries.²⁷ South Africa is, however, gradually increasing the number of extradition agreements, and there are also several treaties currently being negotiated.²⁸

²¹ *Ibid.*

²² National Prosecuting Authority Annual Report for the 2019/2020 financial period, 36.

²³ *Ibid.*

²⁴ *Ibid.*

²⁵ *Ibid.*

²⁶ Luke Feltham “Interpol issues red notices against Guptas and associates” (5 July 2021) < <https://mg.co.za/news/2021-07-05-interpol-issues-red-notices-against-guptas-and-associates/> > accessed 9 August 2021.

²⁷ Department of Justice and Constitutional Development < <https://www.justice.gov.za/ilr/mla.html> > accessed 12 August 2021.

²⁸ Peter Fabricus “SA-UAE treaty does not mean Guptas will be on the next plane home from Dubai” Daily Mail (11 June 2021) < <https://www.dailymaverick.co.za/article/2021-06-11-sa-uae-treaty-does-not-mean-guptas-will-be-on-the-next-plane-home-from-dubai/> > accessed 9 August 2021.

The most notable example of South Africa's increase in extradition efforts is evident from the recent ratification of the extradition treaty ('Treaty') between South Africa and the United Arab Emirates. The NPA recently announced that it has, with the assistance of Interpol, issued red notices on members of the Gupta family with the Treaty having the potential effect of aiding in their extradition. The Gupta family are central in the State's investigative efforts regarding State Capture, with the effect that they are now classified as wanted fugitives. The arrest and extradition of the Gupta's will constitute a benchmark of the efficacy of South Africa's publicly declared zealous pursuit of those instrumental in State Capture.²⁹

Conclusion

South Africa faces significant challenges in recovering even a small fraction of monies and assets illegally dissipated across borders.

Recent precedent does, however, constitute a significant expansion of our courts' jurisdictional reach. This is coupled with increasing publicly-available evidence in the Zondo Commission, as well as civil forfeiture orders being well established in South Africa. As such, the public and private sector have a far more equipped foundation upon which to tackle offshore asset recovery.

²⁹ *Ibid.*

About the Authors

Michael-James Currie is Director of Primerio. Michael's expertise includes complex commercial litigation (including cross border) and dispute resolution before the superior courts including arbitration. Michael is an active member of the ICC's Fraudnet, the world's leading asset recovery group, Michael-James is well versed with the anti-corruption laws in Southern Africa as well as the UK Bribery Act and the Foreign Corrupt Practices Act. Michael-James' practice in this area includes conducting internal investigations, compliance, litigation and asset recovery. Mike currently serves as the International Bar Association Anti-Corruption Committee's regional representative for Africa.



Contact Michael-James Currie: T. +27 (0)11 083 2413; E. m.currie@primerio.international



John Oxenham is Co-founding Principal Director of Primerio, John has practised in the global investigations, regulatory, commercial litigation and antitrust fields locally and across the African region for over 20 years. He has been recognized as a leader in his field for many of these. Recently, John represented Business at the OECD as the first regional representative from Africa. John has acted in many of the leading precedent setting global investigation matters. John is the sole South African representative for FraudNet the ICC's Commercial Crime Division.

Contact John Oxenham: T. +27 (0)11 083 2412; E. j.oxenham@primerio.international

Jemma Muller is a junior at Primerio currently awaiting admission as a legal practitioner. Jemma has regulatory and commercial law practice experience across several African countries and regional blocs including Botswana, Kenya, Namibia, Nigeria, South Africa, Eswatini and COMESA.



Contact Jemma Muller: T. +27 (0)11 083 2416; E. j.muller@primerio.international

Akhmedova v Akhmedov - a case study in successfully dealing with difficult defendants

Anthony Riem and Andrew McLeod

Abstract

In this article, Anthony Riem and Andrew McLeod, Senior Partner and Associate at the London firm of PCB Byrne LLP, review the recent litigation in the judgment of Mrs Justice Knowles in the Family Division of the High Court in *Akhmedova v Akhmedov* [2021] EWHC 545, [2021] 4 WLR 88 (Fam), and the lessons that can be learned about dealing with a recalcitrant defendant in civil fraud proceedings. Such defendants seek to ignore their obligations to the Court or even actively frustrate the Court's orders and processes. Such litigation conduct might be seen in the short term to have benefits, in disrupting or even derailing claims against them. Yet the various powers of the English court to grant interim remedies enable it to interrogate a defendant's claims and if necessary find other methods to compel a defendant to comply with their obligations. These present not only the ability to counteract a defendant's efforts to defeat the court's processes, but the opportunity to convert that litigation conduct into a successful outcome at trial.

Introduction

“All happy families are alike, each unhappy family is unhappy in its own way. With apologies to Tolstoy, the Akhmedov family is one of the unhappiest ever to have appeared in my courtroom”.

Thus began Mrs Justice Knowles her judgment in *Akhmedova v Akhmedov* [2021] EWHC 545, [2021] 4 WLR 88 (Fam). Her quote of *Anna Karenina* is more than a nod to the parties' Russian heritage; it reflects the troubled history of a high-profile divorce where every step was taken to try to prevent the enforcement of a 2016 financial remedy order granted by the Family Division of the High Court of Justice in favour of Tatyana Akhmedova.

Two of the Respondents, Counselor Trust Reg and Sobaldo Establishment (trust entities based in Liechtenstein) simply refused to disclose a single document which was not already in Ms Akhmedova's possession.¹ Another respondent, Borderedge Limited, was alleged to have backdated documents to support an otherwise hopeless defence. Further, Temur Akhmedov was found to have "*lied to this court on numerous occasions; breached court orders; and failed to provide full disclosure of his assets*" and to be "*a dishonest individual who will do anything to assist his father*" in his scheme to put every penny of his wealth beyond Ms Akhmedova's reach.²

Yet despite such aggressive and obstructive litigation conduct, Ms Akhmedova was overwhelmingly successful against respondents who were all found to have deliberately failed to comply with their disclosure obligations.³

However, that ending was not written in stone at the outset. While the trial itself was condensed into fewer than three weeks, and concluded in a result that the judge could summarise in 3 short paragraphs, it was the culmination of over 18 months of procedural wrangling in courts, both domestic and foreign, against not only the Respondents but various related and unrelated third-parties. Between his joinder to the proceedings on 20 January 2020, and giving his evidence in early December 2020, Temur in particular had been made subject to a suite of civil orders to compel or obtain disclosure. Each of these contributed in some small way to the documents at trial, his physical presence at the trial, and ultimately the judgment against him.

This article presents the proceedings against Temur as a case study in the use of interim applications and the English court's coercive powers to compel such a defendant to produce documents that may be used to obtain a judgment against them.

Background

The background to the case rests in the marriage between Ms Akhmedova and Farkhad Akhmedov in Russia in 1993. Ms Akhmedova issued her petition for divorce on 24 October 2013 and applied for financial remedies on 25 October 2013. A financial remedy hearing was heard by Haddon-Cave J between 28 November and 15 December 2016. The Husband's main identified assets were (i) a superyacht known as the M/Y Luna, purchased in February 2014 for €260 million, (ii) a collection of modern artworks valued in January 2016 as US\$145.2 million and (iii) cash and securities worth around US\$650 million (known throughout the proceedings as "the

¹ *Akhmedova v Akhmedov & Ors (Rev 1)* [2021] EWHC 545 (Fam), [2021] 4 WLR 88 at [131].

² *Ibid*, [6].

³ *Ibid*, [130].

Monetary Assets"). By his judgment handed down on 15 December 2016, Mr Justice Haddon-Cave (as he was then) awarded Ms Akhmedova an amount equal in value to the total sum of £453,576,152.

Mr Akhmedov had submitted to the jurisdiction of the English court in the financial remedy proceedings as confirmed by a letter dated 18 June 2015 from his then solicitors, Sears Tooth. However, Mr Akhmedov failed to appear at the November 2016 hearing.⁴ Instead, and unbeknownst to Ms Akhmedova, Mr Akhmedov had implemented a scheme that was intended to make the assets invulnerable to enforcement, by immediately before and during the trial transferring the Monetary Assets, the modern art collection and the Luna into a Liechtenstein trust structure. The scheme was discovered immediately after the trial by cross-examination of Mr Akhmedov's lawyer and "man of business", Anthony (Andy) Kerman of Kerman & Co. Mr Akhmedov then entered into a global effort to resist enforcement, describing it publicly as a war that he would "*continue to fight for as long as it takes, and in whatever jurisdiction necessary*" to resist a judgment he graphically described as "*worth as much as toilet paper*".

Ms Akhmedova's claims in England

Ms Akhmedova's claims were aimed at obtaining English judgments against third parties who had received assets from Mr Akhmedov as part of his evasive schemes prior to and following the judgment. Her claims were brought under s.423 of the Insolvency Act 1986, as well as making use of the Court's (close to) equivalent powers in the family law context, pursuant to s.37 of the Matrimonial Causes Act 1973, as transactions that should be set aside as having been made for a purpose of frustrating or impeding enforcement.

As regards Temur Akhmedov (one of the couple's sons), those transactions related to two categories of assets Temur received for no consideration and for the purpose, at least in part, of protecting them from enforcement by Ms Akhmedova against Mr Akhmedov. The first was a total of approximately US\$100 million, received between 2014 and 2019 from Mr Akhmedov and his companies, derived from the Monetary Assets. The second was the beneficial ownership of a property located on Solyanka Street in central Moscow (known simply as the "Moscow Property") with a value of £6.58 million, transferred to him from Mr Akhmedov in June 2018 (just as Ms Akhmedova began to escalate her enforcement efforts).

Ms Akhmedova's claims against the Liechtenstein trust entities, Counselor Trust Reg and Sobaldo Establishment, and a Cypriot company owned by the couple's sons,

⁴ *Akhmedova v Akhmedov & Ors (Injunctive Relief)* [2019] EWHC 1705 (Fam) at [7].

Borderedge Limited, related to assets received by those entities as part of the 2016 transfer of the Monetary Assets into the Liechtenstein trust structure.

Obtaining disclosure from other sources

Ms Akhmedova started at somewhat of an advantage, having obtained documents from a variety of sources both in England and overseas, including the following:

- Immediately following the judgment in 2016, documents were obtained from Mr Akhmedov's advisors from his solicitor, Mr Kerman, pursuant to an order for production of documents regarding the modern art collection and the Monetary Assets - in relation to these transactions, Mr Justice Haddon-Cave found that Mr Kerman had been acting as a "man of business",⁵ and the Court of Appeal held that no privilege attached to his communications with those third parties.⁶
- Ms Akhmedova was provided with documents that had been in the possession of one of Mr Akhmedov's former advisers, Mr Ross Henderson - while they contained a number of privileged communications, Ms Akhmedova was granted permission to use those documents pursuant to the iniquity exception.⁷
- In 2018, Ms Akhmedova was able to inspect files relating to criminal investigations for fraudulent bankruptcy and money laundering in Liechtenstein, consisting of documents obtained by the Public Prosecutor and submitted to the Court as part of those investigations - this included records of the various trusts' bank accounts and transactions.⁸
- Information was obtained pursuant to orders obtained from the US District Court for the South District of New York pursuant to 28 US Code paragraph 1782, which entitled Ms Akhmedov to conduct discovery aimed, in summary, at identifying international US dollar transactions to /from entities known to be associated with Mr Akhmedov which had cleared through banks based in New York.⁹

This information provided a partial picture of Mr Akhmedov's activities between 2015 and the trial.

⁵ *Z v Z and others (Legal Professional Privilege: Fraud Exemption)* [2016] EWHC 3349 (Fam), [2017] 4 WLR 84.

⁶ *Kerman v Akhmedova* [2018] EWCA Civ 307, [2018] 4 WLR 52.

⁷ *Akhmedova v Akhmedov* [2019] EWHC 3140 (Fam), [2020] 4 WLR 15.

⁸ *Akhmedova v Akhmedov & Ors (Rev 1)* [2021] EWHC 545 (Fam), [2021] 4 WLR 88 at [23].

⁹ *Akhmedova v Akhmedov & Ors* [2019] EWHC 2561 (Fam) at [28].

Interim application: worldwide freezing order

The purpose of a worldwide freezing order is not disclosure-based - it is only intended to prevent a defendant from putting assets beyond the reach of possible judgment creditors. However, the Court's jurisdiction also carries with it the power to make whatever ancillary orders are necessary to make it effective. These include disclosure about the location of relevant property or assets or information about such assets which are or may be the subject of an application for a freezing injunction: CPR Part 25.1(1)(g), *AJ Bekhor & Co v Bilton* [1981] 1 QB 923. The value of this ancillary disclosure in fraud proceedings cannot be overlooked.

In this case, a without notice worldwide freezing order was obtained after Ms Akhmedova learned that Temur had taken steps to actively dissipate an asset subject to one of Ms Akhmedova's claims - namely the Moscow Property. Ms Akhmedova claimed that the Moscow Property had been transferred to Temur for no consideration so as to make enforcement more difficult. Shortly following proceedings being commenced against him in 2020, and in steps deliberately concealed from both Ms Akhmedova and the Court, Temur dissipated that asset by transferring it back to Mr Akhmedov. Mrs Justice Knowles considered this to justify a worldwide freezing order against Temur's assets up to US\$120 million (approximately the amount of Ms Akhmedova's claims) and - importantly - ancillary orders compelling Temur to disclose of his worldwide assets (the "WFO").

That ancillary disclosure was of some significance. Not only did it identify other assets which were subject to the WFO, it also enabled other deficiencies in Temur's disclosure to be identified - in particular, his bank account records identified the existence of further email and storage accounts with Google and Amazon that had not been disclosed pursuant to Temur's disclosure statement or the forensic examination order (discussed below).¹⁰

In addition, the WFO resulted in Temur seeking to mortgage a property at One Hyde Park, London he beneficially owned, and which he claimed was his only asset of value, for the purpose of financing his participation in the proceedings. A variation to the WFO was agreed which made Temur's ability to raise funds conditional on making asset disclosure - this functioned as a mechanism to compel his compliance with the ancillary disclosure order. In addition, Temur was required to obtain the consent of Ms Akhmedova to the mortgage, and disclose documents relating to the funding. It was the course of that disclosure that Ms Akhmedova identified the basis for a search order executed against that property - so, while the WFO was only a "but for" cause of the search order, it is a demonstration that an opponent forced to move may make mistakes.

¹⁰ *Ibid*, [139].

Finally, the general effect of this vivid episode was clear from the judgment, with Mrs Justice Knowles stating that “[h]is behaviour was thoroughly dishonest and casts a long shadow over his case as a whole”.¹¹

Breach of disclosure obligations

The starting point - and the keystone to the cascade of interim applications that followed - was Temur’s deficient disclosure. In July 2020, his disclosure was served. It contained none of his own documents,¹² save for two discrete emails from 2013 (which he believed to be helpful to his case),¹³ and did not cover most of the period in issue.¹⁴ His disclosure statement stated that he had carried out a search on a handful of devices and email accounts. The disclosure statement also explained that Temur had previously had relevant documents in important categories, but that these documents were no longer in his control because they had been destroyed, ostensibly for “*security reasons*”.¹⁵

In the course of the interim applications to follow, it became apparent that this disclosure was woefully deficient, and the non-disclosure was a deliberate decision. Such calculated non-disclosure is not unusual where a defendant may assume they can frustrate or at least weaken a claimant’s case by withholding documents. Other Respondents in the proceedings took much the same approach - the Liechtenstein Trusts “*simply refused to disclose a single document which was not already in the Wife’s possession*”,¹⁶ which the Court described as a flagrant disregard of its orders and as “*nothing but a device to avoid revealing documents unhelpful to their case*”.¹⁷ Regardless, the lack of disclosure provided an opening for the use of the Court’s other powers to interrogate any purported explanations for the non-disclosure, to expose that the true position, and to compel disclosure.

¹¹ *Ibid*, [326].

¹² *Akhmedova v Akhmedov & Ors (Rev 1)* [2021] EWHC 545 (Fam), [2021] 4 WLR 88 at [134].

¹³ *Akhmedova v Akhmedov & Ors* [2020] EWHC 3005 (Fam) at [23].

¹⁴ *Ibid*, [134].

¹⁵ *Ibid*, [133].

¹⁶ *Ibid*, [131].

¹⁷ *Ibid*, [132].

Interim application: Forensic Examination Order

Immediately following Temur's disclosure and his claim not to be able to access relevant documents, Ms Akhmedova applied for and obtained a delivery-up order, requiring that Temur deliver up his electronic devices, and access to four Google-hosted email accounts, to an independent forensic expert (Stroz Freidberg, an Aon subsidiary). Aon were then to assess what (if any) data was accessible or recoverable and whether it appeared relevant data had been deleted and/or otherwise destroyed - what eventually became known as the Forensic Examination Order. Such an order is available in circumstances where the Court is seeking to ensure a party is complying with their disclosure obligations (including, for example, in relation to the asset disclosure provisions of a freezing order), and to confirm whether documents said to have been irretrievably destroyed can in fact be retrieved. With Temur openly admitting to have destroyed documents likely to be significant to the issues in the proceedings, the order could hardly be opposed.

Temur's response was to further frustrate the order.¹⁸ Having purported to arrange his devices to be delivered to Aon by DHL, the parcel "*mysteriously disappeared prior to reaching DHL's warehouse*".¹⁹ Temur later admitted to having masterminded a plan to use an employee to "lose" a parcel containing an old device, so as to provide a false excuse for his non-compliance with that order,²⁰ which became the subject of a police investigation in France.²¹

He also claimed to be unable to remember the password or recovery details for his Google accounts. This was despite Aon's efforts to access them revealing that Temur had deleted one of his account in August 2020 - that is, after the making of the Forensic Examination Order and at a time when he claimed to have been unable to access that account at all.²² Regardless, another route to the emails would be required.

While Google were willing to produce non-content information (i.e. email header information) if served with a US subpoena, it declined to produce content information (i.e. the emails themselves) unless Temur followed their account recovery process - which he was "unable" to do. As a result, a motion to the US District Court was brought seeking an order compelling Google to produce the emails in the named accounts to Aon. To support that application, Mrs Justice Knowles

¹⁸ *Ibid*, [138].

¹⁹ *Ibid*, [138].

²⁰ *Ibid*, [141](c).

²¹ *Ibid*, [138].

²² *Ibid*, [138].

ordered Temur to execute signed mandates authorising and instructing Google to release his emails to Aon.

This was not an immediate fix. First, incredibly and “*without justification*”, Temur instructed US counsel to intervene in opposition to Ms Akhmedov’s motion,²³ and Google opposed the motion with an argument that it could not be compelled to produce the emails based on the Stored Communications Act 18 U.S.C. § 2701. However, with a further order of Mrs Justice Knowles compelling Temur to withdraw his opposition, and separately confirming to the US District Court that in no uncertain terms the English court required its assistance in producing the emails, Google were finally ordered by the US District Court to produce the emails in Temur’s accounts.

Regrettably, with Google launching further (unsuccessful) appeals, the emails were not obtained until after the hearing had commenced and were not ultimately made available for trial. Regardless, those documents would have (subject to an order of the Court) been available for review and use in enforcing a judgment against Temur or the other Respondents.

Interim application: Anton Piller / Search Order relief

As noted above, in late October 2020 - barely two months out from the trial - Ms Akhmedova received from Temur’s solicitors a valuation report for the One Hyde Park flat, as part of his efforts to obtain her consent to mortgage for his funding. The photographs of that flat showed a number of electronic devices in Temur’s study - devices which plainly fell within the scope of the Forensic Examination Order, yet had not been disclosed by Temur.

Anton Piller / Search Order relief is a draconian measure²⁴ - similar to a private search warrant - and sits at “*the extremity of the court’s powers*”.²⁵ It has been described as one of the court’s “*nuclear weapons*”.²⁶ As with a worldwide freezing order, the purpose is preservation, not disclosure - it enables the seizing of evidence to prevent its destruction, and it does not *per se* permit any information, documents and/or data to be inspected and used. However, such an order may enable access to a source of relevant evidence that otherwise would not have been disclosed.

In this case, the execution of the search order did just that. A significant number of computers, phones, and storage devices - 47 in number - were found when the

²³ *Ibid*, [139].

²⁴ *JSC BTA Bank v Ablyazov (No 1)* [2015] UKSC 64; [2015] 1 WLR 4754 at [19].

²⁵ *Anton Piller K.G. v. Manufacturing Processes Ltd* (1976) 1 All E.R. 779 at 784 (C.A.).

²⁶ *Bank Mellat v Nikpour* [1985] FSR 87 per Donaldson LJ at 92.

Search Order was executed, which contained “*a mass of relevant documents*”.²⁷ Those documents included some relating to distributions to Mr (Farkhad) Akhmedov’s bank accounts from the Liechtenstein Trusts (dating from 2017), which was of significance to rejecting Temur’s claim to have been unaware of any transfers from the Trusts to Mr Akhmedov after 2016.²⁸ In addition, it exposed that Temur had failed to reveal devices in contempt of the Forensic Examination Order,²⁹ and was another example of his persistent and deliberate breaches of the court’s orders.

Bringing Temur to the jurisdiction, and an eleventh-hour reversal

The final stages of pre-trial process showed perhaps the significant results that can arise where a defendant witness is required to attend court in person for the giving of their evidence.

The process of bringing Temur into the courtroom began prior to the pre-trial review two months out from the trial, where Ms Akhmedova sought (and obtained) an order not only ordering Temur to physically attend the trial to give factual evidence and be cross-examined in person, but requiring his legal representatives confirm his travel to the jurisdiction (or presence in a quarantine-exempt country) in advance of the trial, so as to comply with quarantine requirements.

Regardless, despite having purchased a plane ticket to London, Temur did not arrive. On the first of the Court’s reading days, his solicitors applied to come off the record as Temur had been unable to obtain his mortgage - a result of his failure, in Ms Akhmedova’s eyes, to satisfy the disclosure requirements imposed by the WFO Variation. On the first day of the trial, he appeared by video-link in Russia, unrepresented, without funding, and “*begged for help*”.³⁰ In the words of Mrs Justice Knowles, “*the court was faced with a deeply unattractive scenario for the impending trial...[t]hat struck me as wholly contrary to the interests of justice*”.³¹ Instead, a solution was crafted - Temur was allowed to raise finance against the property, conditional on his making disclosure as to the matters Ms Akhmedova claimed were outstanding, and returning to the jurisdiction.³²

Even then, he still failed to comply with the Court’s order to disclose identified documents. Despite being ordered to produce proper information on the investments and transactions of a business in which he was heavily involved, he simply cherry-

²⁷ *Akhmedova v Akhmedov & Ors (Rev 1)* [2021] EWHC 545 (Fam), [2021] 4 WLR 88 at [136].

²⁸ *Ibid*, [280].

²⁹ *Ibid*, [136].

³⁰ *Ibid*, [155].

³¹ *Ibid*, [156].

³² *Ibid*, [156].

picked a small number of emails.³³ Regardless, his attendance at court had been procured. His attendance in the jurisdiction meant he had no choice but to produce a laptop and iPhone that he should have surrendered pursuant to the Forensic Examination Order. These devices produced further significant documents for use at trial, including apparent evidence of Temur and Borderedge’s corporate directors backdating documents.³⁴

Finally, immediately before giving his oral evidence, Temur produced two fresh witness statements. The first contained admissions which the judge described “*on any analysis ... constituted persistent and deliberate breaches of court orders*”.³⁵ He admitted he had failed to give “full” disclosure in breach of the Court’s various orders, and admitted his role in the disappearance of the DHL package.³⁶ In addition, the night before his oral evidence began, a second witness statement was filed. This made wholesale amendments to an earlier witness statement setting out his factual evidence for the trial, in places completely reversing his previous position on his knowledge of, and role in, Mr Akhmedov’s schemes of evasion.

These witness statements were presented as the culmination of Temur’s “*come to Jesus moment*”, when he “*finally saw the error of his ways and wished to assist the Court by giving honest evidence and complying*” with the Court’s orders.³⁷ The Court ultimately rejected this. Explanations he gave were dismissed as “*utter nonsense*”, and instead Knowles J regarded the timing of the admissions “*as entirely of a piece with his unscrupulous litigation conduct in the months before trial*”.³⁸ Indeed, it is hard not to draw the conclusion that any change was triggered by the prospect of the judge’s penal powers over witnesses giving evidence in her courtroom.

Significance of the disclosure, and lessons learned

The significance of the documents produced was particularly evident in Knowles J’s conclusion on Temur’s oral evidence, which she described as “*extremely illuminating*”.³⁹ It was indeed “*the opportunity to view him giving evidence over a prolonged period*” that satisfied Mrs Justice Knowles that he was not a witness of truth, and had in fact lied in various aspects of his evidence.⁴⁰ That conclusion was the product of careful cross-examination to attack his credibility, with Temur taken

³³ *Ibid*, [144].

³⁴ *Ibid*, [366].

³⁵ *Ibid*, [142].

³⁶ *Ibid*, [142].

³⁷ *Ibid*, [144].

³⁸ *Ibid*, [142].

³⁹ *Ibid*, [177].

⁴⁰ *Ibid*, [173].

to inconsistencies between his evidence and the documentary evidence that had been obtained through that disclosure.

In addition, where various orders failed to produce complete or even any disclosure, they instead produced before the Court a clear picture of Temur's litigation conduct, which by the time of his oral evidence formed a catalogue of contempt. Ultimately, given the content of Temur's oral evidence, Mrs Justice Knowles considered it unnecessary to rely on any adverse inferences from this litigation conduct in coming to her conclusions.⁴¹ Regardless, it is not difficult to see how producing a narrative of contempt will influence the course of proceedings. This might not only arise in a judge's approach to successive interim applications - in this case, this was perhaps most obvious in Mrs Justice Knowles' willingness to make what amounted to an informal request to the US District Court to assist Ms Akhmedova's motion and bring documents before the English court in the face of repeated and open obstruction by Temur - but also in the eventual outcome, in circumstances where (as in this case) a party's defence may be "*dependent upon my finding him to be a witness of truth*".⁴²

The case showed the way the Court's various powers can be used by a claimant seeking to get around a defendant's refusal to comply with disclosure obligations. Other possibilities include various methods to obtain disclosure from third parties. Domestically, this includes applications of non-party disclosure under CPR 31.17, issuing witness summonses under CPR 34.2 to produce documents to the court and/or attend Court to give evidence, and the use of the Court's powers to issue *Norwich Pharmacal* or *Bankers Trust* orders. When overseas defendants introduce an international angle to proceedings, there may be a wide range of other options available in other jurisdictions, with benefits coming to those who can find creative methods to obtain documents that are admissible in English proceedings.

The case also showed the momentum that can be created by successive interim applications. While each had a distinct purpose, they were interlinked both in narrative and effect. Disclosure from one assisted upon the other - the Forensic Examination Order was sought on the basis that it would assist with Temur's compliance with the WFO, while the WFO disclosure in turn identified breaches of the Forensic Examination Order. In addition, applications frustrated by Temur gave rise to new ones. The Forensic Examination Order, flouted by Temur's "forgetting" his passwords, gave rise to the US motion to compel Google to produce the content of those accounts. At times, new applications arose in unintended ways, such as the Search Order produced from the disclosure pursuant to Temur's efforts to raise funding. Ultimately, those applications and the resulting disclosure provided the

⁴¹ *Ibid*, [177].

⁴² *Ibid*, [173].

Court with all the context it needed to determine the claims in favour of Ms Akhmedova.

However, the case also shows that these efforts are ultimately a race against the clock. Temur's efforts to frustrate access to documents, including obstructing access to his Gmail accounts, were in part successful as whilst it did not impact upon the outcome of the trial, they were not available for use at the trial. Such emails could, possibly, have found a use in later enforcing the judgment (should that have proven necessary), which provides a further reason to push on. However, efforts to obtain disclosure can play into a defendant's hands if they seek to slow down progress or even use them as the basis to seek an adjournment under the guise of needing time to comply. Claimants need to balance the value of obtaining these documents against the risks of prejudicing their ability to proceed with a trial, and the need to maintain momentum in the proceedings. That momentum is crucial not simply to exert pressure on defendants, but in order to maintain the stamina and willingness of all participants to continue to engage, when to do so feels like (with this time an apology to Fyodor Dostoevsky) its own personal *Crime and Punishment*.

Ms Akhmedova was represented by PCB Byrne LLP (Anthony Riem, Rachel Turner, Andrew McLeod, Catherine Eason, Caitlin Foster) and funded by Burford Capital.

About the Authors



Anthony Riem is a Senior Partner at PCB Byrne LLP. Over the past 30 years, Anthony has established himself as a leading lawyer in fraud investigation and asset recovery, having deep expertise in handling complex cross-border disputes. Strategically-minded and a source of astute, commercially-focused advice, he has a long-standing practice acting for financial institutions, government agencies and high net worth individuals in multi-million dollar litigation.

Anthony is double Ranked in Band 1 by Chambers for Global-wide Asset Tracing and Recovery and Civil Fraud, and named as a Leading Individual for Civil Fraud by the Legal 500 and a Global Thought Leader for asset recovery in Who's Who Legal. In 2021, he was named as one of Britain's most sought-after lawyers by The Times and one of the 100 Hot Lawyers by The Lawyer Magazine.

Contact Anthony Riem: T. +44 (0)20 7842 1616; E. ariem@pcb-byrne.com

Andrew McLeod is an Associate at PCB Byrne LLP. Andrew is an adept commercial litigator with experience across a wide range of high-value civil fraud and commercial disputes.

With a focus on complex civil fraud proceedings - covering both substantive trials, foreign enforcement of judgments and applications for urgent interim relief - Andrew's career has also seen him work on challenging commercial disputes, fraud and regulatory investigations and anti-money laundering matters. Andrew is identified by the Legal 500 2022 edition as a "key lawyer for Commercial Litigation".



Contact Andrew McLeod: +44 (0) 20 7842 1616; E. AMcLeod@pcb-byrne.com

Ransomware Relief: A Review of the Development and Use of Norwich Pharmacal Orders in Ireland

Joanelle O’Cleirigh

Abstract

In this article, Joanelle O’Cleirigh, Partner at Arthur Cox, Dublin, examines the use of a Norwich Pharmacal order as part of the Irish State response to the recent cyberattack on the Irish public health care service and its evolution as a tool to provide redress against cyberattacks.

Introduction

In May 2021, the Irish public health service was the subject of an aggressive ransomware cyberattack which forced the shut-down of its IT systems and had a massive impact on the Irish health care system. Described by an Irish government minister “*as possibly the most significant cybercrime attempt against the Irish state*”¹, the abhorrent attack crippled the Irish health service and led to a compromise of the delivery of healthcare and also the potential misuse of sensitive personal data. The disruption to the Irish health service was very significant and it is ongoing².

In the aftermath of the ransomware attack, the Irish public health service successfully secured injunctive relief against the unidentified perpetrators. Following the discovery that stolen files had been placed on a malware analysis service called VirusTotal which is owned by Chronicle Security Ireland Ltd and its

¹ J Horgan Jones, S Burns, C Lally & P Cullen, ‘Bitcoin Ransom will not be paid following cyber attack on HSE Computer Systems’, *The Irish Times*, 14 May 2021 available at: <https://www.irishtimes.com/news/health/bitcoin-ransom-will-not-be-paid-following-cyber-attack-on-hse-computer-systems-1.4564957> accessed 12 October 2021

² ‘HSE Cyber Security Incident Update’ last updated 29 July 2021, <https://www.hse.ie/eng/services/news/media/pressrel/hse-cyber-security-incident-update.html>, accessed 27 August 2021

US-based parent Chronicle LLC, both of whom are ultimately owned by Google, the Irish public health service procured Norwich Pharmacal orders against Chronicle Security Ireland Ltd and Chronicle LLC to require the disclosure of details of those who uploaded or downloaded the stolen information³.

This article traces the evolution of Norwich Pharmacal orders - from their original conception as a response limited to tortious wrongs, to a legal device approved by the Irish courts to aid the identification of the perpetrators of cyber-attacks and to limit the harm flowing from such attacks. While the ambit of Norwich Pharmacal orders in England and Wales has reached far beyond the threshold outlined in the original case, in Ireland the courts have exercised greater restraint in the development of the Norwich Pharmacal order as an avenue of equitable relief.

Origins of the Norwich Pharmacal Order

A Norwich Pharmacal order is a type of disclosure order compelling a person with knowledge of the identity of wrongdoers to disclose that information.

A relatively recent legal innovation, it was first granted less than 50 years ago in the English decision in *Norwich Pharmacal Co. v Customs and Excise Commissioners*⁴ wherein it was held:

*“If through no fault of his own a person gets mixed up in the tortious acts of others so as to facilitate their wrong-doing he may incur no personal liability but he comes under a duty to assist the person who has been wronged by giving him full information and disclosing the identity of the wrong doers.”*⁵

In this seminal case the plaintiffs obtained an order compelling the defendant to reveal the details of importers who, through statistics published by the defendants, were revealed to be importing a chemical compound in alleged infringement of the plaintiff’s patent.

The jurisdiction to grant a Norwich Pharmacal order was first recognised in Ireland by the Supreme Court in *Megaleasing UK Ltd v Barrett*.⁶ While a Norwich pharmacal order was not granted by the Supreme Court, it held that a plaintiff must establish a *prima facie* case of wrongdoing to secure a Norwich Pharmacal order.

³ A O’Faolain, ‘Orders granted requiring Google owned firms to provide detail of identities’, The Irish Times, 29 June 2021, available at <https://www.irishtimes.com/news/crime-and-law/courts/high-court/orders-granted-requiring-google-owned-firms-to-provide-detail-of-identities-1.4606829> , accessed 12 October 2021

⁴ [1974] AC 133.

⁵ *ibid* 175.

⁶ [1993] ILRM 497.

Development of the scope of Norwich Pharmacal Orders in England and Wales

In the aftermath of the decision in *Norwich Pharmacal*, the scope of the Norwich Pharmacal order developed in England and Wales. Soon after the Norwich Pharmacal judgment was handed down, *British Steel Corporation v Granada Television Ltd*⁷ clarified that the plaintiff pursuing a Norwich Pharmacal order need not intend to institute legal proceedings against the wrongdoer. This same principle was reiterated in *Ashworth Security Hospital v MGN Ltd*,⁸ which further extended the ambit of Norwich Pharmacal orders in holding that such orders can be pursued for all forms of wrongs, not only tortious wrongs.

In contrast to the approach adopted by the Irish courts in its later decision in *Megaleasing UK, in P v T Ltd*⁹ the courts in England and Wales broadened the scope of Norwich Pharmacal orders almost to the nature of fact finding. In this case, the plaintiff's employer had dismissed him for gross misconduct based on third party allegations which had been made against him but they refused to explain what the misconduct was, leaving the plaintiff unable to explain himself to potential future employers. Having brought a successful claim to the industrial tribunal, the defendant was ordered to re-engage the plaintiff which it refused to do. The plaintiff's employment prospects were seriously hindered as it was known within the industry that he had been dismissed for alleged impropriety however as the plaintiff did not know what was alleged against him, he could not clear his name. The court deemed it to be 'in the interests of justice' that the plaintiff be entitled to such information and granted the application for a Norwich Pharmacal order. While this judgment could be limited to the merits of this particular case, it demonstrated the attitude of the English courts who favoured the grant of a Norwich Pharmacal order for a wide variety of reasons.

In *R (Mohamed) v Secretary of State for Foreign and Commonwealth Affairs (No 1)*,¹⁰ the court considered the test of necessity and held that a Norwich Pharmacal order should only be granted where it is satisfied that the information being sought was necessary. However, the court held that this does not mean that there must be no other practicable means of obtaining that information. When considering necessity, it was held that the court was to have regard to various circumstances, including the plaintiff's resources, the urgency of the need for the information, public interest in the application and proportionality.

⁷ [1981] AC 1096.

⁸ [2002] UKHL 29.

⁹ [1997] 4 All ER 200.

¹⁰ [2009] 1 WLR 2579.

In *Rugby Football Union v Consolidated Information Services Limited (formerly Viagogo Ltd)*¹¹, an English decision which pre-dated the EU's General Data Protection Regulation, the court considered the balancing of rights between the victim of the wrong and the right to privacy of the wrongdoers, noting the need to have regard to the following factors:

1. the strength of the possible cause of action contemplated by the applicant for the order;
2. the strong public interest in allowing an applicant to vindicate his legal rights;
3. whether the making of the order will deter similar wrongdoing in the future;
4. whether the information could be obtained from another source;
5. whether the respondent knew or ought to have known that he was facilitating arguable wrongdoing;
6. whether the order might reveal the names of innocent persons as well as wrongdoers, and if so whether such innocent persons will suffer any harm as a result;
7. the degree of confidentiality of the information sought;
8. the privacy rights under article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms of the individuals whose identity is to be disclosed;
9. the rights and freedoms under the EU data protection regime of the individuals whose identity is to be disclosed; and
10. the public interest in maintaining the confidentiality of journalistic sources.

In *Rugby Football Union*, ultimately the contractual rights of the plaintiff won out over the wrongdoers' rights to confidentiality.

In *Various Claimants v News Group Newspapers Ltd & Ors*¹² the court considered the extent to which the defendant must be 'mixed up' in the wrongdoing. In this action the plaintiffs were seeking a Norwich Pharmacal order against the police for information they held on the matter. The information involved was held by the police as part of their investigation into the matter. The police were held to have been more than a "mere witness" to the wrongdoing, a category which had been expressly precluded from the order in the original *Norwich Pharmacal* case. A

¹¹ [2012] UKSC 55.

¹² [2013] EWHC 2119 (Ch).

Norwich Pharmacal order was granted in a decision which arguably expanded the scope for Norwich Pharmacal orders to be made against any party with material information surrounding the wrongdoing.

Evolving remedy in Ireland

In Ireland the courts have exercised greater restraint in the development of the Norwich Pharmacal order as an avenue of equitable relief.

The Irish High Court decision in *EMI Records (Ireland) Ltd & Ors v Eircom Ltd and BT Communications Ireland Limited*,¹³ first signalled the evolution of Norwich Pharmacal orders in this jurisdiction to meet the challenges of the new millennium. This was the first notable case of a Norwich Pharmacal action being taken against an internet service provider in Ireland. The plaintiffs were seeking information on parties who had illegally downloaded copyrighted music, to which the plaintiffs held the sole rights in this jurisdiction, and had infringed their copyright. As the music had been pirated by parties who were connected to the internet via the defendants' service, the Norwich Pharmacal order was sought against the defendants to disclose the pirates' identities. It was held that, while the court should have respect for the pirates' right to confidentiality, whether it considers that right to have arisen by statute, at common law, or by virtue of their contracts with the defendants, that right to confidentiality cannot be relied upon by a wrongdoer to protect their identity. The court made a Norwich Pharmacal order however it was conditional on the provision by the plaintiff of an undertaking that the information disclosed by the defendant would not be used for any purpose other than seeking redress in respect of the infringement of copyright the subject of the proceedings.

The Irish courts have continued to apply the principle that there needs to be *prima facie* evidence of wrongdoing for the threshold for a Norwich Pharmacal order to be met with the courts conducting a balancing exercise in order to assess whether the balance of justice favours the grant of a Norwich Pharmacal order. In *Parcel Connect Limited Trading as Fastway Couriers and A & G Couriers Limited v Twitter International Company*¹⁴ the court heard an application for a Norwich Pharmacal order directing the defendant to disclose information it held in relation to the identity of the person or persons who created and/or controlled an account on the social media platform operated by the defendant. The plaintiffs claimed to be wronged by various entries posted on this account which had been set up using the plaintiff's trade name and the Fastway logo, which is a registered trademark. The court summarised the legal principles with respect to the burden of proof, noting that "*the judgments in Megaleasing UK Ltd. spoke of a threshold test that the*

¹³ [2005] IEHC 233.

¹⁴ [2020] IEHC 279.

plaintiff was required to establish a very clear and unambiguous case of wrongdoing, but as Humhpreys J. recently explained in the High Court in *Blythe v. Commissioner of An Garda Siochana* [2019] IEHC 854, certainty or a high degree of certainty is not required. Rather it is sufficient, as Kelly J. put it in *EMI Records Ireland Ltd. v. Eircom Ltd.* [2005] 4 I.R. 148 that the plaintiff should make out a *prima facie* case of wrongful activity, or as Ryan P. put it in *O'Brien v. Red Flag Consulting Limited* [2017] IECA 258, a strong *prima facie* case.”¹⁵ On the facts, the court was satisfied that the plaintiffs had established a strong *prima facie* case that, inter alia, the plaintiff’s goodwill in their name and mark had been damaged and that the postings wrongly and maliciously held the plaintiffs up to ridicule. Following the *EMI Records Ireland Ltd* decision, the court made the Norwich Pharmacal order conditional on the provision of an undertaking that the information disclosed by the defendant would be solely used for the purpose of seeking redress in respect of the wrongdoing complained in these proceedings.

The decision in *Muwema v Facebook Ireland*¹⁶ is notable for Facebook successfully arguing against a Norwich Pharmacal order due to the exceptional circumstance of the wrongdoer’s life potentially being in danger. The court held that the right to life and bodily integrity of another must take precedence over a person’s right to his good name where the threat to bodily integrity is sufficiently serious.

In the very recent decision in *Board of Management of Salesian Secondary College (Limerick) v Facebook Ireland Limited*¹⁷ proceedings were brought by a school board of management to compel the social media platform, Instagram, to disclose the identity of individuals behind one of its user accounts which had made a series of posts mocking and insulting the plaintiff school and its staff. The school’s board of management were of the view that the account users were either students or staff members at the school and wanted to identify the individuals for the purposes of “dealing with” them through a “disciplinary or pastoral response”. The school authorities initially requested the data from Facebook through correspondence. Facebook advised that it could not disclose the information without a court order or request from law enforcement. At the time of the institution of the proceedings, the user account was inactive and the relevant posts had been deleted. Facebook adopted a neutral position in respect of the proceedings.

The court ultimately concluded that it was necessary to make a reference to the European Court of Justice for a preliminary ruling on certain issues with respect to privacy, data protection and freedom of expression. The court noted the particularly striking aspect of Norwich Pharmacal orders is that the party whose identity it is intended to reveal are not on notice of the proceedings. Thus, if the order is granted,

¹⁵ Ibid 5.

¹⁶ [2018] IECA 104

¹⁷ [2021] IEHC 287

it is too late for them to challenge the decision, as the full relief will have been obtained. This is further exacerbated as the defendant party, as was the case here, will usually take a neutral position and not defend the rights of the third party.

The Irish court emphasised the importance of the duty of candour of the applicant due to the absence of a *legitimus contradictor*. The court held that this duty created an obligation to put all material facts before the court and to identify the relevant legal principles governing the court's jurisdiction, including any EU law principles.

The court stipulated that it must be satisfied of the threshold conditions for the grant of disclosure, including:

1. The disclosure is necessary for, and proportionate to a legitimate aim.
2. The affidavit and grounding application must explain the precise purpose for which the disclosure order is sought.
3. If granted, a disclosure order will be made conditional on an undertaking that the information disclosed will not be used for any purpose other than seeking redress in respect of the wrongs complained of.

The court attributed significant weight to the fact that, in this case, the information was not sought for the purpose of instituting proceedings and thus the court was being asked to depart from the established requirement that an applicant seeking a Norwich Pharmacal order must intend issuing legal proceedings for tortious wrongdoing. The court acknowledged the scope to expand the jurisdiction to grant Norwich Pharmacal orders in Ireland, referencing the recent decision in *Grace v. Hendrick*¹⁸ wherein a disclosure order was granted in reliance on the court's inherent jurisdiction despite the lack of *prima facie* evidence of wrongdoing in that particular case.

The court took the view that the rights afforded to privacy, data protection and freedom of expression under EU law potentially placed a limit on the scope to expand the jurisdiction to grant Norwich Pharmacal orders in Ireland and decided to make a reference to the European Court of Justice. However, the applicant ultimately withdrew its case and thus the questions raised by the Irish courts have not yet been resolved.

This judgment was distinguished in a more recent decision in *Portakabin Limited and Portakabin (Ireland) Limited v Google Ireland Limited*¹⁹ which concerned an application for a Norwich Pharmacal order in order to identify the person or persons responsible for sending emails to the plaintiffs' customers which were alleged to be

¹⁸ [2021] IEHC 320.

¹⁹ [2021] IEHC 466.

defamatory and damaging to the plaintiff's interests. The plaintiffs' aim in seeking to establish the author of the emails was to issue legal proceedings against them for damages and, if the author transpired to be an employee of the plaintiffs, take disciplinary steps against that person. The court noted that the *Board of Management of Salesian Secondary College* case could be distinguished as in that case the disclosure sought was not for the purpose of issuing proceedings but rather for the purposes of "dealing with" the authors of the posts through a "disciplinary or pastoral response". The court concluded that the substance of this *Portakabin* case was a claim of wrongful damage to the plaintiffs' business and reputation and therefore it fell within the established jurisdiction to grant a Norwich Pharmacal order. The court granted the order on the plaintiffs' undertaking that the information provided on foot of the order would only be used to institute and pursue legal proceedings seeking redress in respect of the emails complained of or if the author transpired to be an employee, for the purposes of taking disciplinary steps against that person.

Commentary and Outlook

The success of the very recent application by the Irish health care service to secure a Norwich Pharmacal order in the context of the recent ransomware attack confirms the willingness of the Irish courts to move beyond the confines of tortious wrongdoing and permit the expansion of the doctrine where the balance of justice favours granting relief. There remains a question whether issues around data protection, privacy and freedom of expression under EU law will be introduced and lead to a referral to the ECJ that proceeds.

Internationally condemned, the ruthlessness of both the target of the attack and its timing in the midst of the Covid-19 global pandemic has highlighted the growing global risk posed by ransomware attacks. As such, the Irish courts have accepted the role of the Norwich Pharmacal order as a practical tool to identify wrongdoers in the cybercrime sphere and limit the harmful consequences of their actions.

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.



Contact Joanelle O'Cleirigh: E. joanelle.ocleirigh@arthurcox.com

Enforcement of Foreign Judgments in Lebanon

Nada Abdelsater

Abstract

Enforcement of foreign judgements is key in asset recovery. Indeed, even the best judgment is of little use if it cannot be enforced. In this article, Nada Abdelsater, founding Partner of ASAS Law, provides a high-level description of foreign judgement enforcements in Lebanon with the view of shedding some light on relevant questions and processes to be considered when developing the right legal and strategic approaches to enable efficient recovery.

Brief legal overview

The enforcement process of a foreign judgment in Lebanon starts by granting the said judgment exequatur by the competent Lebanese court. In the asset recovery world, speed and surprise are of the essence. Even prior to completing its exequatur, the foreign judgment may be used before the Lebanese courts, to obtain conservatory measures such as legal guardianship, provisional seizures and other.

Various conventions and international treaties relating to enforcement of foreign judgments are ratified or signed by Lebanon, for example:

- The Judicial Convention between Lebanon and Italy, signed on 10 July 1970 and ratified by law dated 17 May 1972.
- The Convention for the Mutual Judicial Assistance and Enforcement of Judgments and Extradition Between Lebanon and Tunisia, signed on 28 March 1964 and ratified by law dated 30 December 1968.
- The Convention Concerning the Enforcement of Judgments Between Lebanon and Kuwait, signed on 25 July 1963 and ratified by law dated 13 March 1964.

- The Judicial Agreement between Lebanon and Jordan, signed on 31 August 1953 and ratified by the law dated 6 April 1954.
- The Judicial Agreement between Lebanon and Syria, signed on 25 February 1951 and ratified by law dated 27 October 1951.
- The Arab Agreement for Judicial Cooperation, signed by members of the League of Arab States on 18 February 1953 - Lebanon signed but did not ratify.
- Finally, Lebanon also recognizes foreign arbitral awards in accordance with the terms of the relevant conventions to which Lebanon has acceded; for example Lebanon is member to the 1958 New York Convention on the Recognition and Enforcement of Arbitral Awards.

Final vs. Interim or Temporary Foreign Judgments

Put briefly, the Lebanese Code of Civil Procedure ('LCCP') has set conditions that must be met so that foreign judgments may be enforced. Generally speaking, foreign judgments that have not acquired "authority of a final and irrevocable judgment" (*res judicata*) and enforceability in the originating country, may not be enforced in Lebanon. If interim/temporary decisions and ex parte decisions have become enforceable in the originating foreign country, Lebanese courts would grant such decisions *exequatur*.

Enforcing Foreign Judgments

As mentioned above, in general, the process of enforcing a foreign judgment in Lebanon starts by seeking the "exequatur" decision from the relevant Lebanese court. The foreign judgment must comply with the following cumulative conditions set out by Article 1014 LCCP:

- The foreign judgment must have been issued by competent judges in accordance with the law of the foreign originating country, provided that their competence is not strictly determined based on the nationality of the claimant.
- The foreign judgment must have already acquired "authority of a final and irrevocable judgment" (*res judicata*) and enforceability in the foreign country. However, Lebanese courts may grant *exequatur* to interim/temporary decisions and ex parte decisions if they have become enforceable in the foreign country.

- The condemned must have been notified of the lawsuit which entailed the foreign judgment and its rights of defence must have been ensured.
- The foreign judgment is rendered by a state permitting the enforcement of Lebanese judgments on its territory after due examination or exequatur (the principle of reciprocity).
- The foreign judgment does not violate the public order.

The submission of an exequatur request for a foreign judgment is made *ex parte*, to the President of the competent Civil Court of Appeal depending on the domicile or the location of the respondent or the place of the assets to be seized. Otherwise, the President of the civil Court of Appeal of Beirut would be competent.

Another condition is for the exequatur request to be filed by a lawyer admitted to practise in Lebanon; the following documents must be submitted with the exequatur request:

- a certified copy of the foreign judgment satisfying all validity conditions according to the originating foreign country;
- the documents proving that the foreign judgment has acquired enforceability according to the originating foreign country (*res judicata*);
- a certified copy of the complaint filed against the party that did not attend the trial, and the document evidencing the notification of the trial papers if the award was rendered in absentia;
- a certified and legalised translation of all above documents in compliance with the Lebanese law;
- a valid power of attorney in the name of the lawyer filing the exequatur request.

Once the exequatur is obtained, the foreign judgment may be enforced in the same manner as domestic judgments. The typical compulsory enforcement measure is the “executory seizure” of the debtor’s assets placing them under court custody and eventually selling them in public auction under the authority of the court.

Timeframe

The exequatur request is usually transferred to the President of the Court of Appeal. The President will issue a decision either granting or rejecting the exequatur request; in some cases the judge would issue an interim decision requesting, for

example, further information and documents. The decision-denying exequatur is subject to challenge before the Court of Appeal within a period of 15 days. The decision granting the exequatur is subject to appeal within a period of 30 days as from its notification to the debtor/defendant.

In general, the debtor will be notified of the exequatur decision and the enforcement proceedings at the same time. This would be the time when the debtor would generally appeal the said exequatur decision and try to stop enforcement of the foreign judgment. Indeed, practically speaking, and because the exequatur decision is granted *ex parte*, the creditor will initiate the enforcement proceedings before notification to the debtor.

We outline these separately as they will usually run in parallel before separate courts. With respect to the exequatur appeal proceedings before the court of appeal, these are subject to the general rules applicable to appeals. The appeal decision is usually rendered within a few months¹; however, some proceedings extend much longer. Moreover, the appeal decision itself is subject to the general rules applicable to challenging appeal decisions (cassation, retrial and third-party objection). These challenges would further extend the timeframe needed to enforce the foreign judgment.

As for enforcement, the seizure order may be obtained in one day²; however, the actual attachment and foreclosure proceedings which would result in the realisation of the debt, are much longer and vary on a case by case basis. In some cases, debtors would come forward and pay the debt within the five-day period set by the executive bureau, whilst others would use every potential delay and challenge all possible proceedings; as such, the enforcement proceedings could extend for several months and even years.

From an asset recovery standpoint, the most efficient option to enforce a foreign judgment is to start by obtaining an *ex parte* provisional seizure on the identified assets. As previously mentioned, this has the advantage of surprising the debtor as the decision is rendered without prior notification.

Asset Tracing - How to identify Assets in Lebanon?

There are various ways to identify a person's assets in Lebanon (be it a natural person or a legal entity), subject to the restrictions regarding bank accounts (as outlined in the Lebanese Banking Secrecy Law, dated 3 September 1956). Asset identification

¹ All estimated timeframes mentioned in this article are estimates that would apply in normal times. At the date of drafting this article Lebanon is living an unprecedented economic crisis which consequences are affecting the progress of affairs in the judicial sector and public administrations.

² *Idem*.

methods vary depending on the type of assets, as further detailed below.

A) Shares

Companies in Lebanon are registered at the relevant commercial registry depending on the location of their respective headquarter. The information available in the registry is accessible to the public. In general, the process of gathering information starts by filing a request to obtain a “comprehensive certificate”; this document provides information such as the name of the shareholders, their shareholding, the name of the directors, lawyers, auditors, the address of the company and a record of all judicial attachments on the company. Moreover, the commercial registry has a website where some information is accessible electronically. However, unlike the real estate register, an official search on a “per-person” basis, is not yet available at the commercial registry enabling the identification of the various shares/parts held by an individual or entity in different companies in Lebanon.

This said, it is helpful to note that information on companies and individuals holding interests in companies may be obtained from private search entities for a fee depending on the type of requested reports. Asset recovery lawyers have the requisite knowledge and experience with the various available tracing options. They are best fitted to advise their clients on the most efficient asset tracing strategy to identify the assets of the target.

B) Bank Accounts

In Lebanon, bank accounts and banking information are protected by a special protection layer based on the Law on Banking Secrecy, dated 3 September 1956. There are two levels of protection. Except under special circumstances, a) the banks in Lebanon are subject to “professional secrecy” and b) monies deposited with banks in Lebanon may not be seized. Any violation of the banking secrecy obligation is subject to criminal sanctions involving imprisonment.

In general, banks systematically refrain from giving banking information, even when summoned by the Lebanese Administration or by a Lebanese court order. This said, few exceptions apply to this banking secrecy. For example, such exceptions are outlined in the Banking Secrecy Law and in the Law on Fighting Money Laundering and Terrorist Financing, dated 24 November 2015. Moreover, the Law for the Exchange of Information for Tax Purposes No 55, dated 27 October 2016 allows the communication of fiscal information under international mutual assistance conventions.

According to the Banking Secrecy Law, the banking secrecy is lifted in the following cases:

- when the concerned client, his/her heirs or legatees provide a written authorisation allowing the disclosure of information; or
- if the bank's client is declared bankrupt; or
- if there is a lawsuit involving banks and their clients concerning banking operations.

Moreover, immunity from seizure may be bypassed when it can be proven that it was authorized by the account holder.

Law No 44 on Fighting Money Laundering and Terrorist Financing also provides for cases where the banking secrecy may be lifted in events involving money-laundering. In the event of suspicious transactions, it would eventually be for the Special Investigation Commission (SIC) to receive and analyse the suspicious transaction reports, conduct financial investigations, lift banking secrecy, freeze accounts and/or transactions and forward information to concerned judicial authorities. This is the playground of specialized asset recovery lawyers expert in banking asset tracing.

C) Real Estate Assets

Lebanon has a real estate register department or '*cadastre*' corresponding to regions or departments where real estate properties are registered. The rights pertaining to land or real estate properties are created by registration with the said register. The real estate register is public and the information therein can be accessed by any person. It also has an electronic database accessible to the public.

The process of identifying the assets owned by an individual or a legal entity starts by submitting a request to the General Directorate of Land Registry and Cadastre in Beirut. The search result takes the form of a list showing the properties owned by the target person. This document is typically issued within few days³.

Once the properties are identified, further investigation may be undertaken to gather additional information on each identified plot. In general such enquiry is made with the relevant real estate registry department. An initial start would be to obtain a real estate certificate which provides details concerning the property, including the names of the owner(s) and their

³ *Idem*

respective shares, the property description and records of the securities attached thereto such as seizure, mortgage, lawsuits etc.

Conclusion

In conclusion, Lebanon is a country that recognizes and enforces foreign judgments and is member to various conventions and international treaties relating to enforcement of foreign judgments and arbitral awards. Asset tracing or unveiling “hidden assets” may prove to be particularly useful if the right legal approaches and strategies are put in place prior to embarking on the actual enforcement.

Special Thanks to ASAS partner Me. Serena Ghanimeh for her contribution and collaboration on this article.

About the Author



Nada Abdelsater is an international lawyer admitted to the Courts of New York and Beirut. She is the founding partner of ASAS Law, a Lebanese law firm with activities across the Middle East and extending to Europe, USA and commonwealth countries. She has a strong practice in international cross border transactions, litigation, and arbitration including notably white-collar crimes, as well as complex commercial litigation, confiscation, freezing orders and cross border enforcement of judgements and arbitral awards. Her clients include multinationals and high-profile individuals.

She leads multi-faceted investigation processes and asset recovery proceedings across several jurisdictions according to rigorous and high professional standards. She advises clients on tracing and seizing or freezing funds and assets located in Lebanon or deposited in Lebanese Bank Accounts. She acts for clients in liberating funds that were unduly frozen by international or national regulatory authorities. Nada handles complex transactions including financial engineering, M&A, oil and gas, PPP, corporate and financial transactions and corporate governance restructuring.

Nada is continuously ranked as “Leading Lawyer” by the major reputed international guides. She is the recipient of the Corporate Governance Rising Star Award, 2009, Yale University. She holds a Masters in Law from Harvard Law School, a Lebanese and French Master Law degree from University Saint Joseph in Beirut, a Bachelor of Science from the American University of Beirut and has completed the M.A coursework in International Affairs at the Lebanese American University.

Contact Nada Abdelsater: T. +9611384556; E. nada.abdelsater@asaslaw.com

Hunting for Hidden Treasures in Austria with New Enforcement Rules - What to expect from the “Overall Reform” of Austrian Enforcement law?

Bettina Knoetzl and Katrin Hanschitz

Abstract

In this article, Bettina Knoetzl and Katrin Hanschitz, Partners at Knoetzl, give an overview of the main new concepts introduced into the Austrian Enforcement Code by the recent, relevant, reform bill. After describing the context that triggered the reforms, it summarizes the new bundling of enforcement measures and introduces the administrator as the new player in Austrian enforcement. In closing, the authors consider the advantages of the new regime and how it will change the practice of asset recovery in Austria.

Introduction

As the final step, after three decades of modernization of Austrian enforcement law, the Austrian legislature recently passed a reform bill entitled the “Overall Reform of the Enforcement Code” (*GREx*). The GREx came into force on 1 July 2021. The goal of the GREx is to increase efficiency in the conversion of monetary awards into Austrian assets. To that end, the GREx introduces two entirely new concepts that into Austrian enforcement law:

- the introduction of so-called enforcement “bundles” (see below 2.1) and
- the - almost revolutionary - transfer of powers to a newly created player, the so-called “administrator”, responsible for tracing and realizing upon assets (see below 2.2).

After a short description of the law to date, a summary of the central new rules will be set out.

1. Law to Date

1.1 Enforcement in Austria is court-controlled

Unlike in most other European enforcement systems, the Austrian enforcement system is characterized by the strong involvement of the courts and certain civil servants (bailiffs). Enforcement against a debtor's assets requires prior approval by a court, with the enforcement measures generally being laid out by designated court officers (currently bailiffs). This central concept remains unchanged under the new reform bill. The court will continue to hold the reins.

1.2 Need for change

In cases in which the debtor had easily realizable assets, i.e.

- assets that were easily identifiable from public records, such as the online Land, or the Company, Register, or
- a salary from an ongoing employment,

the existing enforcement mechanism for enforcement against receivables generally proved efficient.

In cases where such assets were not as readily available or identifiable, particularly when savvy debtors concealed their attachable assets, the Austrian enforcement system showed itself to be too cumbersome. Under the rules prior to the GREx, the creditor had to specify exactly which assets against which it wished to enforce its claim.

Private creditors who lack direct access to coercive measures, can be quickly stymied in their search for attachable assets, particularly where debtors are committed to impede any attachment of their assets. Practitioners have long felt that a legal policy that abandons creditors holding enforceable claims to only their own resources like this, is untenable.

- For example, while it has not been necessary to name the debtor's employer when attaching his salary, when creditors attempted to attach any claims a self-employed, or unemployed, debtor may have had against a third party, they were required to *specify* and *individualize* the claim - including, at least, i) the name and address of the third-party debtor, ii) the legal grounds, and iii) the approximate amount of the claim. This information is rarely available to the creditor. Enforcement efforts on a "hit or miss" basis generally come to naught. Repeated applications have burdened the court system and frustrated creditors. The added costs ultimately burden the debtors, provided assets are finally found and realized.

- The situation is similar for bank accounts. A creditor was required to name the specific bank if it wished to attach the debtor's bank account. In view of notably strict Austrian bank secrecy rules, creditors rarely have access to such banking details. This led to creditors often naming a long list of banks as third-parties in the hope that one of the banks would confirm the existence of an account. In the meantime, the creditor was required to advance the costs for each of the bank responses (EUR 25 each).
- Creditors could have, under certain circumstances, demanded that debtors provide an affidavit listing their assets (Sec 47 Enforcement Code, "EC"). Unfortunately, by the time the creditor received the affidavit, the strategy of launching a "surprise attack" was obviated, and the easily realizable moveable assets such as notebooks, tablets, jewelry, watches etc. were simply concealed or disappeared.
- Additionally, creditors only became aware that the debtor, ultimately, had insufficient assets only *after* investing significant resources into the red-herring enforcement measures.

Investing the necessary effort and numerous follow-on applications meant that successful creditors needed to not only have persistence, but also sufficient funds. Less well-healed creditors were often simply unequipped to stay the course.

The good news for creditors pursuing enforcement in Austria after 1 July 2021 is that new measures have been introduced to overcome each of these drawbacks.

2. What does the Reform Bill Change?

In order to increase efficiency and the success rate of enforcement efforts, creditors now have the option of

- choosing "bundled" enforcement measures and
- benefiting from the appointment of an "administrator" (*Verwalter*) as a new and central player in the enforcement proceedings.

2.1 "Bundling" of enforcement measures

While creditors can continue to request targeted enforcement measures against specified assets, they now also have the additional option of requesting either a "small bundle" or an "extended bundle" of enforcement measures.

Neither bundle includes enforcement against immovable property, which remains subject to the “old” regime. Since real estate in Austria is always registered in the Land Register, giving creditors technical and legal access to details of any real property the debtor may own in Austria makes this unproblematic.

2.1.1 The “Small Bundle” Sec 19 EC

This small bundle includes

- enforcement against movable (corporeal) goods and “paper” (i.e. securities) (Sec 249 EC)
- attachment of salary claims against (also unknown) employers (Sec 295 EC), and
- requiring an affidavit, listing assets from the debtor (Sec 47 EC).

Garnishment of a debtor’s salary continues to have priority before the seizure of assets (Sec 249a EC).

The small bundle is structured as the default option and is triggered if a creditor does not specify enforcement measures in the enforcement application. This has the added benefit of simplifying enforcement applications to the court, as the creditor no longer must specify any enforcement measures at all. In the past, courts often returned enforcement applications to the applicant for correction, often because of mistakes in specifying enforcement measures being sought.

The main benefit of the creditor’s utilization of a small bundle is that the court begins acting *automatically* as soon as the enforcement application has been approved, and continues its enforcement efforts until full satisfaction has been achieved (or the debtor is shown to have no assets). Under the old regime, when e.g. insufficient movables were found at one address, or the debtor moved jobs, additional applications by the creditor were generally necessary to advance the enforcement process.

The small bundle option is expected to become a popular form of enforcement, particularly as applied against consumers with few assets.

2.1.2 The “Extended Bundle” Sec 20 EC

In more complex enforcement cases, creditors will presumably favor the so-called “*extended bundle*”. This option is available when the creditor’s enforceable claim exceeds EUR 10,000, and in cases in which the seizure of movable assets is shown to be insufficient.

The extended bundle includes, in addition to the enforcement measures contained in the small bundle, enforcement measures against all movable assets (Secs 249 to 345 EC), including:

- any other receivables the debtor may have against third parties, such as against banks, customers, shareholders etc., and
- any other assets, including claims for delivery of assets or real property, claims to have real property sub-divided, claims against delivery of shares etc.

If the creditor chooses the extended bundle, the court will appoint an enforcement administrator, similar to an insolvency receiver. The administrator has more extensive powers than the traditional bailiff in realizing against assets. For example, the administrator is not constrained by the rule that salary garnishment takes priority over the seizure of assets, and he has full discretion to choose to sell moveable assets directly, rather than through an auction (Sec 249b, 269 para 2 EC).

2.2 The Enforcement Administrator

2.2.1 Overview

Until the GREx, the Enforcement Code provided for “administrators” (receivers) only in cases of compulsory administration of real estate and certain other property rights. The GREx has introduced the concept of a *general* administrator for all types of enforcement in order to streamline proceedings, by concentrating knowledge, specialized skills and specialized powers into one person.

Once appointed by the court, the administrator will first identify available assets. For this purpose, he can communicate directly with the debtor, who is obliged to provide information to the administrator, including any necessary documents, PIN-Codes, Krypto currency “keys” etc., required to realize claims against the assets, to provide access to his place of business, any storage facilities and, most importantly, to his books and records (Sec 81 EC). The administrator may also require an affidavit on the assets. Failure of the debtor to cooperate can lead to penalties, and even imprisonment by the enforcement court.

After drawing up an inventory, the administrator will choose which assets upon which to realize first - i.e. which assets will most quickly and comprehensively satisfy the creditor(s)’ claims. He will subsequently attach and realize upon the chosen assets until the creditor(s)’ enforceable claims have been satisfied. In this context, the administrator has many of the powers bailiffs currently have, with the exception of unlocking locked residential doors.

There is a small fly in the ointment for particularly active creditors, specifically: subsequent creditors who request the extended bundle against a debtor join the pending “bundle” enforcement proceedings at the *status quo*, with the same administrator acting for all creditors, as would an insolvency receiver. Quick-acting creditors, nonetheless, still benefit because proceeds are distributed according to priority.

In contrast to counsel, the administrator must act objectively (Sec 27 para 3 EC), but has autonomy to choose which methods and measures of enforcement he believes are most suitable. Indeed, administrators have more flexibility and, in some areas, more powers than bailiffs (Sec 81 para 9; also Sec 249b and 268 para 3 EC).

The court nonetheless retains control of the enforcement proceedings throughout the process: The administrator is bound by instructions issued by the court and is subject to the court’s ongoing supervision (Sec 84 EC). If administrators fail to properly discharge their duties, they can be fined by the court and, moreover, be held liable by creditors (Sec 81a EC).

Creditors can generally waive the appointment of an administrator if they wish to enforce against specific, identified assets. There are exceptions, in particular where the enforcement measures involve the sale or compulsory administration of a business or company or of real property, in which cases administrators are compulsory. The administrator’s far-reaching powers may prove problematic for a creditor in certain circumstances: For example, if the creditor is co-shareholder of the company that is to be sold, he cannot prevent the administrator from taking measures that could collaterally damage the creditor, such as instigating the dissolution of the company. The fact that the administrator is required to provide information on the planned method of realization 14 days in advance (Sec 81 para 5 EC) does, however, give the creditor the opportunity to explore alternative realization methods with the administrator and, if necessary, make a clarifying application to the court.

2.2.2 Qualifications

Enforcement administrators are registered on a central list administered by the Higher Regional Court in Linz.

Applicants must substantiate that they are well-suited for the function as administrator. Relevant criteria include experience in commercial, civil and enforcement law, as well as necessary management, IT and accounting skills together with the necessary organization and office equipment to enhance rapid recovery. The legislature envisaged lawyers, business consultants and auditors serving in this role. (Sec 79 et seq EC). Insolvency receivers will presumably be among the first to be registered as administrators.

2.2.3 Costs

Administrator's fees are staggered (generally between 15% and 1% of the amount recovered). The minimum amount, EUR 500, will be advanced by the creditor before the administrator can be instructed (Sec 82 EC). Since the creditor no longer needs to file multiple applications, the additional fees for the administrator are not expected to make the proceedings more expensive for creditors.

3. Conclusion and Outlook

Practitioners anticipate that the GREx will increase the efficiency of many enforcement proceedings, with the new system of bundling enforcement measures sparing creditors the laborious supervision of enforcement measures, and the necessity of numerous follow-on applications. The trade-off is that creditors will have to advance some higher costs. However, since administrators are paid a percentage of the realized proceeds, it is hoped that the new system will more than pay for itself, in view of the administrator's extensive powers and access to coercive measures against unwilling debtors.

Ultimately, the quality of administrators will be instrumental in determining how successful the new extended bundle system becomes. Creditors with large claims and tricky debtors would do well to rely on experienced asset recovery experts to enable effective recovery in collaboration with the administrator. Experience, expertise and good judgment and, where necessary, persistence in dealings with courts, bailiffs and administrators will remain critical factors in determining the success of enforcement measures under GREx.

About the Authors



Bettina Knoetzl is the exclusive Austrian representative of the ICC FraudNet and a founding partner at KNOETZL, a leading law firm specialized on dispute resolution, asset tracing and white-collar crime work. In 2017, Bettina was given worldwide recognition and named “Lawyer of the Year” in Asset Recovery by Who’s Who Legal, London.

She is a passionate trial lawyer with 25 years’ experience in international and national matters of high profile, scoring notable successes in commercial litigation, fraud and corruption matters including criminal defence work. Bettina is the President of Transparency International (Austrian Chapter), Vice President of the Lawyers’ Bar, Vienna, and the past IBA Co-Chair of IBA’s global Litigation Committee (2016-17) and a member of the Business Crime Subcommittee focusing on Asset Tracing.

Contact Bettina Knoetzl: T + 43 1 34 34 000 200; E. bettina.knoetzl@knoetzl.com

Katrin Hanschitz is a partner with KNOETZL and works as an experienced first-chair litigator in international corporate and commercial litigation, crossing over into white collar crime, enforcement and insolvency as dictated by clients’ needs. Recent cases include complex cross-border disputes in the banking, construction, energy and life sciences industries as well as in new technologies and international trade.



Contact Katrin Hanschitz: T. +43 1 34 34 000 700; E. katrin.hanschitz@knoetzl.com



ICC FraudNet
Global Annual Report 2022

PART THREE

THE OFFSHORE DIMENSION

No Stone Unturned: Tools of the trade available to the asset recovery lawyer in Guernsey

John Greenfield, David Jones and Robin Gist

Abstract

The Bailiwick of Guernsey has long been determined to avoid being labelled a "black hole" for ill-gotten gains to be secretly stashed away. In this article, John Greenfield, David Jones and Robin Gist of Carey Olsen Guernsey set out the weapons at the disposal of the asset recovery lawyer - many of which will have a familiar ring about them. Some however, perhaps less so. This article analyses the methods available to extract the information that any claimant needs from other parties (reluctant or otherwise); obtaining of pre-emptive Court Orders to preserve assets that have been uncovered; assisting actions in other jurisdictions and finally bringing into play the full might of an insolvency practitioner with all the powers at their disposal.

Knowledge

The old adage that "knowledge is power" is particularly relevant and appropriate here. It is essential to any successful investigation to be able to consider and understand as much of the relevant documentation as it is possible to track down. The tools available to a Guernsey lawyer for obtaining such information include:

- (a) Third party disclosure:
 - (i) Norwich Pharmacal Orders;
 - (ii) Anton Piller Orders;
 - (iii) Bankers Trust Relief with Freezing Orders;
 - (iv) Bankers Books Orders.

- (b) Mutual international assistance:
 - (i) The Commission Rogatoire;
 - (ii) International judicial assistance and cooperation;
 - (iii) Foreign insolvency and cross border cooperation.

- (c) Disclosure and specific disclosure in the course of proceedings;

(d) Entitlement to inspect documents referred to in pleadings etc.

We shall be taking a brief look at each of these remedies and processes. It should be noted that many of these applications are often heard 'In Camera', but many important principles have been established and are widely understood in the Royal Court of Guernsey ('the Court').

Third Party Disclosure

The principles established in Guernsey are very similar to those in England and Wales and other Commonwealth jurisdictions - save that there is no formal pre-action protocol procedure and (at least in asset recovery cases) there is no formal pre-action disclosure. However, the following remedies are available to obtain early disclosure:-

1. Norwich Pharmacal Orders

The Court in Guernsey will apply the principles set out in the House of Lords decision in *Norwich Pharmacal v. Commissioners of Customs and Excise* (1974) UK HL6, per Lord Reid:

"If through no fault of his own a person gets mixed up in notorious acts of others so as to facilitate their wrongdoing he may incur no personal liability but he comes under a duty to assist a person who has been wronged by giving him full information and disclosing the identity of the wrongdoers. I do not think that it matters whether he became so mixed up by voluntary action on his part or because it was his duty to do what he did... justice requires that he should co-operate in righting the wrong if he unwittingly facilitated its perpetration".

A typical scenario involving Guernsey would be where corporate vehicles which are administered in Guernsey (and may be Guernsey registered companies) and have a corporate service provider resident in Guernsey are used by a wrongdoer in another jurisdiction to facilitate the transfer of funds in the hope that they would become out of reach of the victim.

A Norwich Pharmacal application is particularly relevant where the victim needs to identify the appropriate defendant or defendants to his substantive action. The Royal Court has imposed some limitations on the scope of this type of application - notably by the Court of Appeal in Guernsey in the case

of *Systems Design Limited v. Equatorial Guinea (President)* 2005-2006 GLR page 65. This was a case arising out of the unsuccessful coup to overthrow the president of Equatorial Guinea by Simon Mann and others where it was alleged that funds to assist the coup had been, or were being, held in Guernsey and the President wished to identify those persons responsible. The application failed for a number of reasons but the Court took the opportunity to lay down some principles including:

- (a) The application must not be merely for the purpose of obtaining pre-trial discovery of what a witness might say if called at trial;
- (b) The third party with the relevant information must have become involved in the wrongdoing but not to such an extent that such third party could or should be joined as a party to the substantive proceedings - indeed, it may be, and usually is, wholly innocent;
- (c) The applicant must identify the wrongdoing about which the complaint is made;
- (d) The information sought can include identifying the wrongdoers, seeking to understand the existence or nature of the wrongdoing and also the location of assets upon which a judgment might be enforced;
- (e) The "wrongdoing" must be such as to be recognised as wrongful in the eyes of the law, whether criminal conduct or the infringement of a civil right which the law can protect;
- (f) It is not a condition that the applicant must have started or intend to start civil action in respect of the wrongdoing. It is enough that he has a legitimate interest to protect whether by way of seeking redress or by lawfully preventing further wrongdoing;
- (g) The applicant has to identify the purposes for which the disclosure will be used when made so that the Court will be able to restrict such use if necessary;
- (h) The power towards discovery is discretionary and must be deemed to be "*essential and necessary*" to assist him in achieving justice.

2. Bankers Trusts Orders

Again the Royal Court in Guernsey has confirmed that it would follow the principles established by the Court of Appeal in England and Wales in the case of *Bankers Trust v. Shapira and Others* (1980) 1 WLR 1274 to enable the Court to order disclosure of information not only to identify a wrongdoer, but also to enable a plaintiff to trace assets that had allegedly been obtained by fraud. In such, there must be:

- (a) Strong evidence of fraud - such orders go against the normal rules of confidentiality so cannot be made lightly, and it is the evidence of fraud which militates against the usual confidentiality principles;

- (b) Good grounds for asserting that the assets in question belong to the applicants; and
- (c) A demonstrable need for urgent action.

The Royal Court has further extended the ambit of such orders in the case of *Seed International Limited v Tracey*, unreported, 3 November 2003 and approved by the Court of Appeal on the 18 December 2003. In this case it was stated that the Court should exercise its power to grant such orders not only in relation to proprietary claims but also to personal claims where it is just and convenient in all other circumstances of the case to do so.

3. Anton Piller Orders

An Anton Piller Order again has been granted (but not frequently) by the Court to allow a party (usually under appropriate supervision) to search, inspect and seize documents or property (whether stored in files physically or electronically on computers) relating to infringement of the applicant's rights or otherwise relevant to his claim. This remedy is available in cases where: *"...Plaintiffs had a very strong prima facie case actual or potential damage to them was very serious and there was clear evidence the Defendants possessed vital material which they might destroy or dispose of so as to defeat the ends of justice before any application inter partes could be made, the Court having inherent jurisdiction to order Defendants to "permit" Plaintiffs representatives to enter Defendants premises to inspect and remove such material"*.

The Royal Court will normally hear such an application In Camera, ex parte and without notice. This application has to be made with care as it is only justified to interfere with a parties' normal rights and liberties where the objectives could not be made by an order for delivery up or preservation of documents, computers, etc. The applicant will normally have to give an undertaking in damages as a condition of being granted any such order.

4. Bankers Book Orders

Further, in this particular group of remedies, The Bankers Books Evidence (Guernsey) Law, 1954 provides a discrete mechanism for the inspection and copying of entries in bankers books. Once again, it is a discretionary remedy and the Court is expected to balance the principles of confidentiality with the interests of justice.

5. Disclosure once substantive proceedings have commenced in Guernsey

Standard Disclosure:

Once proceedings have been commenced, then the normal and standard duties of preserving and disclosing information and documents will apply. Disclosure forms a key part of civil proceedings in Guernsey and is largely modelled on the regime established by the Civil Procedure Rules in England and Wales - except that the Guernsey Rules are much less voluminous and prescriptive than their counterpart in England and Wales, which can often be to a litigator's advantage.

Each party must provide a list to the other disclosing the existence of all documents which are now (or ever have been) in their "possession, custody or power" and are relevant to the issues in dispute.

The obligation to give disclosure must be made thoroughly and conscientiously as there are severe sanctions if a party to legal proceedings fails to comply fully with this obligation. Documents that are "privileged" are exempt from this obligation. Certain documents that have been or will be created will be privileged or withheld from inspection, the most important categories being:

- (a) Legal advice privilege; documents or correspondence between the client and members of the legal profession for the purpose of giving instruction or obtaining legal advice. This covers almost all communications between the client and its lawyers;
- (b) Litigation privilege; documents where the dominant purpose for which the document was created was to obtain legal advice or to collect evidence in respect of contemplated or ongoing litigation.

The disclosure process is a continuing one and applies to documents which may be created in the future. Generally disclosure under this process means that such documents may only be used for the purpose of the proceedings within which it has been disclosed.

In the complex commercial cases often now appearing before the Royal Court, it has been used to applications being made by a party to whom the document belongs to nevertheless restrict or even prohibit any further use of the document and/or, in the opposite, faces an application to the Court for permission to use such documents in other proceedings where they are clearly relevant. Like many other important legal principles, this exception was grappled with by the Court recently in the *re Tchenguiz Discretionary Trust* (2017) *unreported* judgment 3/2018.

6. Specific Disclosure

Any party to proceedings may apply to the Court for Orders requiring an opposing party to make "specific disclosure" of a document if there is a real probability that the document sought will, on inspection, yield information of a substantial evidential materiality to the case as pleaded at the time of the application. Blanket orders will not be granted on the mere possibility of a fruitful train of enquiry being revealed - see *James L Smith v. Islands Insurance Company Limited* (Royal Court Judgment 2001/28) and *Norman Piette Limited v Hochtief Constructions (UK) Limited* 2005 GLR 50.

7. Disclosure of a Document referred to in Pleadings

An often overlooked weapon is Rule 73 of the RCCR, which sets out the potentially extremely useful resource available to demand sight of documents referred to in any formal Court documents including pleadings, witness statements, affidavits or expert reports. This power will extend not merely to documents which have been specifically and expressly identified in the Court documents but also where they are alluded to and can be identified from that reference. This always has to be subject to the principles of proportionality and in the past the Court has refused such requests where the pleading referred to merely identified "a room full of documents" at a specific address.

8. Arret Conservatoire

This power is available to conserve assets pending the outcome of a hearing. It provides the customary power to freeze assets where a creditor wishes to arrest a specific identifiable tangible asset of personal property located in Guernsey - the fruits of which may ultimately be used to satisfy a prospective judgment. It is distinguishable from the injunctive relief/freezing orders which require a respondent not to deal with assets generally. The Arret Conservatoire is designed to preserve assets where otherwise a claim will be worthless where:

- (a) The plaintiff has a cause of action in Guernsey against a defendant (this can be via reciprocal enforcement of a foreign judgment);
- (b) The defendant has property in Guernsey which is capable of arrest. This applies only to personalty e.g. money, boat, planes, etc., and in relation to claims for liquidated sums - not realty;
- (c) There are good grounds for believing that without this arrest it is likely the goods will be removed from Guernsey and the plaintiff will suffer prejudice in attempting to recover the debt.

This procedure can be used against third parties who hold property for the debtor.

9. Freezing Orders

The Court in Guernsey has all the usual powers available to the Courts of England and Wales to grant orders of injunctive relief to a claimant pre-action whether limited to assets in Guernsey or worldwide freezing orders.

The usual requirements for such orders have been set out by the Court, namely:

- (a) The claimant has a good arguable case against the respondent;
- (b) There is a real risk that any judgment the claimant may obtain will go unsatisfied by reason of the disposal of assets unless the respondent was restrained; and
- (c) It is just and convenient in all the circumstances for the freezing injunction (and the ancillary orders) to be made including an order to prevent abuse.

Such an order may well be ancillary to substantive proceedings in Guernsey or elsewhere. If the order is sought ancillary to proceedings elsewhere then:

- (a) The Court may well expect that the primary court will have already granted such relief; and
- (b) The applicant must identify both:-
 - (i) the actual or prospective proceedings in aid of which the application is made;
 - (ii) the prospective judgment whose enforcement the defendant is not to be permitted, by dissipating its assets, to frustrate.

The Court has stated that once the prerequisites are fulfilled then the Court should not be timid in granting freezing orders that are needed to protect plaintiffs whether at home or abroad from having future judgments rendered valueless by the dissipation of the defendant's assets. See *Garnet Investments Limited v. BNP Paribas (Suisse) SA*, Guernsey judgment 2/2009, paragraph 89.

10. Assisting other jurisdictions

The Commission Rogatoire:

By the Evidence (Proceedings in other Jurisdictions) (Guernsey) Order 1980, the provisions of the Evidence (Proceedings in other Jurisdictions) Act 1975 are extended to the Bailiwick of Guernsey. The Court has authority pursuant to that Act to assist the High Court of England and Wales to obtain evidence from residents or institutions in Guernsey.

The Hague Convention on the taking of evidence abroad in civil or commercial matters 1970 was extended to Guernsey in 1981. The Court may also assist High Courts in other Hague Convention states (which includes most of the EU, USA, Australia, China, UK, etc) to obtain evidence within Guernsey for the purposes of civil proceedings which have been instituted before that other Court or are contemplated before that Court. However, the procedure cannot be used for a pre-trial disclosure of documents, per Article 23 of the Convention.

In relation to any application received, Guernsey Courts must use the same procedural laws with regard to the collection of evidence - it will be for the foreign Court to ultimately rule on its admissibility. In Guernsey, an application for assistance by a foreign Court is known as a Commission Rogatoire - by which evidence can be taken in Guernsey for use in foreign proceedings and visa versa in foreign jurisdictions for use in Guernsey.

The first step is to obtain a "letter of request" (letter rogatory) from the relevant foreign court. Usually this will be sent directly to an Advocate who prepares an application to the Court. The following details must be included in the letter rogatory:

- (i) Details of the action which has been commenced or is contemplated;
- (ii) Questions to be asked of the witness or subject matter of the questioning;
- (iii) List of documents the witness is required to produce or property to be inspected.

The Court must be satisfied that the application is made in pursuance of a request issued by a foreign Court. It can order the provision of documentary evidence, but will not grant an order requiring a witness to state what evidence he has had in his possession, custody or control - as this would amount to a

fishing expedition which would not be permissible - see *Rea Brothers (Guernsey) Limited v. SEC* (1986) 3 GLJ 22. If the application is granted, a commissioner, usually an officer of the Royal Court in Guernsey (called a 'jurat') is appointed to preside over the proceedings. A date is fixed for the Commission Rogatoire and the witnesses are formally summonsed to appear.

11. General Assistance to other proceedings

Disclosure will be ordered by the Court in appropriate cases to assist foreign proceedings providing the Court considers it "just and convenient". This jurisdiction extends to making disclosure orders ancillary to freezing orders - even where no proprietary claim is an issue.

12. Foreign Insolvency Provisions

As the fallout from the restrictions imposed by governments around the world to protect against the spread of COVID-19 begins to manifest, many believe that a wave of insolvencies is coming. In some cases those insolvencies will expose financial wrongdoing leading to insolvency practitioners riding the crests of complex fraud investigations.

The suite of information gathering powers afforded to insolvency practitioners should always be kept in mind when seeking information. In many jurisdictions, the insolvency office holder's powers will go some way beyond those available to members or creditors of an insolvent entity. Naturally, those insolvency practitioners with a background in asset tracing will also have available to them, often in-house, expertise in forensic accounting, e-disclosure and data analytics that can be brought to bear in investigations. Consequently, there can be value in exploring the possibility of considering making formal insolvency appointments to an entity involved in an investigation to help crack open the door.

Whilst the mechanisms by which appointments could be secured in Guernsey are outside of the scope of this article, our article for last year's publication, entitled 'Creditor's Rights and Remedies in Guernsey', explored that detail and may be worth revisiting.

However, it is not just domestic Guernsey appointments that are worthy of consideration when looking for information held here. Guernsey's Royal Court has an established record of assisting foreign office holders in the performance of

their duties, including information gathering and we now look briefly at the routes to recognition in the coming paragraphs.

Recognition can essentially be divided into two types. First, section 426 of the UK Insolvency Act 1986 has been extended to Guernsey by the Insolvency Act 1986 (Guernsey) Order 1989. The effect of this is that the Royal Court can provide judicial assistance to the courts of England and Wales, Scotland, Northern Ireland, the Isle of Man or Jersey in insolvency matters. Equally, Guernsey officeholders are entitled to seek assistance in those jurisdictions that have chosen to elect Guernsey as the specified country for incoming requests.

A letter of request issued under these provisions is authority for the receiving court to apply either its own insolvency law (or the insolvency law of Guernsey) and, in the event, its own jurisdiction and powers. Section 426(5) states that the receiving court "shall assist" the requesting court and the UK courts have granted assistance in a wide variety of circumstances. This is a powerful tool and would allow an insolvency practitioner to utilise his full suite of domestic information gathering powers in the reciprocating jurisdiction including, for example, section 236 powers granted under the Insolvency Act 1986.

The second type of recognition is under the common law. This is an area that has been subject to substantial development in other jurisdictions in recent decisions, particularly that of the Privy Council in *Singularis*. The key to common law relief is often the information gathering powers an office holder in the receiving jurisdiction would be afforded under its own laws. Guernsey continues to develop its domestic laws and, in particular, expects to introduce revisions to its law this year that will increase the investigative powers of office holders.

In any event, the broad position is that Guernsey will cooperate in foreign insolvency proceedings, particularly where there is a sufficient connection between an officeholder appointed in the jurisdiction where the company is incorporated or individual domiciled and the company or individual has submitted to the jurisdiction of the court where the appointment was made. Although the Royal Court still retains discretion under the common law, where there is a sufficient connection the Court will typically grant the relief sought.

Conclusion and Outlook

As stated at the outset of this article, Guernsey is keen to ensure it is not perceived as some form of ‘tax haven’ where the proceeds of a fraud can disappear. In the case of *Seed International Limited v Tracey*, it was stated that when exercising the Court’s discretion in this type of application the Court had to bear in mind the special circumstances of a small island community and the need to maintain the highest standards of probity for its financial services industry. The speed at which assets can be transferred out of Guernsey worldwide made it appropriate in the circumstances to maintain an order for the disclosure of information. The Island is determined that victims of fraud should not be left powerless if the perpetrators sought to use any of the services available in Guernsey’s finance industry to avoid detection or justice.

About the Authors

John Greenfield is a Consultant in the dispute resolution and litigation group 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 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 member of the Committee that completely overhauled Guernsey’s civil procedure in 2008 and is now part of the new review Committee in 2021. He has been the Guernsey member of the UK Fraud Advisory Panel since 2001.

Contact John Greenfield: T. +44 (0) 1481 732026; E. john.greenfield@careyolsen.com



David Jones is a Partner and head of the restructuring and insolvency team in Guernsey. He advises on complex restructurings and formal insolvencies in contentious, non-contentious and multi-jurisdictional matters. David 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. He regularly advises the boards of distressed entities and has extensive experience acting for office holders on all aspects of their appointments including the tracing and recovery of assets. David 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).

Contact David Jones: T. +44 (0) 1481 741554; E. david.jones@careyolsen.com

Robin Gist, Senior Associate, is an advocate in the dispute resolution and litigation group. He brings a unique mix of significant experience of both the private and public law spheres, including in regulatory and data protection matters. Robin works with both international and local clients on a broad breadth of contentious issues, regulatory matters and general advisory work, including private client and property matters.



Robin is a director of the Institute of Law, Guernsey, a member of the Guernsey Bar Council and sits on the Tax Tribunal. Robin is Deputy Bâtonnier of the Guernsey Bar Council, and he also sits on the Tax on Real Property Tribunal. He has extensive experience of appearing in all the Bailiwick of Guernsey's courts, including the Court of Appeal.

Contact Robin Gist: T. +44(0)1481 732095; E. robin.gist@careyolsen.com

Notes from a Small Island

Colette Wilkins QC, Nick Dunne and Andrew Gibson

Abstract

In this article, Nick Dunne and Colette Wilkins QC, Partners, and Andrew Gibson, Senior Counsel, at the law firm Walkers, based in the Cayman Islands, set out recent developments in Cayman Islands law with particular relevance to the conduct of major cross border litigation and asset recovery.

Introduction

As the sight of cruise ships bobbing in Hog Sty Bay, and the steady stream of aircraft full of holidaymakers touching down at Owen Roberts Airport, rapidly recede into distant memory, it would be tempting to think that life in the Cayman Islands has been on pause for much of the past two years. However, as much as that might be true in some respects, the financial services and legal sectors have each continued apace and uninterrupted. That activity has included a number of significant developments relevant to the world of asset recovery.

The Private Funding of Legal Services Act 2020

Funding asset recovery claims is frequently a complicated issue for lawyers, and historically the Cayman Islands has done little to make that process any easier. In contrast to much of the rest of the common law world, the crimes of champerty and maintenance remained in existence, and the few cases in which the Grand Court had been willing to sanction non-traditional fee arrangements involved terms which were so commercially unattractive as to be unworkable in the context of heavy litigation.

That state of affairs, however, rapidly became unworkable against a background of liberalised funding elsewhere. It offered protection to the fraudster who had succeeded in leaving the cupboard bare and left liquidators of impecunious companies in severe difficulties, no matter how legally sound and valuable the claims vested in those companies. Those problems had led to a discernible softening in judicial attitudes in recent years, but that could only take matters so far in the face of an unhelpful legal landscape.

However, that landscape was fundamentally altered by the enactment of the Private Funding of Legal Services Act, which came into force on 1 May 2021. In addition to sweeping away champerty and maintenance as crimes and torts, the Act now provides a clear statutory framework for the utilisation of both alternative fee arrangements and commercial litigation funding.

First, attorneys are now permitted to accept cases on the basis of contingency fees, an umbrella term which embraces both conditional (or ‘no win, no fee’) arrangements whereby a premium on normal fees is payable in the case of success, and contingency fees where the attorney takes an agreed percentage of the property recovered. The Act caps the maximum success fee at 100% of normal fees in respect of the former, and a third of recoveries in the latter. The Court retains a discretion to approve an arrangement exceeding these caps in appropriate cases, although the standard provisions appear sufficient to cover the vast majority of situations.

Second, funding from third party sources is now permitted in all cases. Whilst the Act contemplates that the content of funding arrangements may, in part, be prescribed in the regulations, they are currently silent in that regard. As such, although the funding must be on terms whereby the cost of the funding must either be calculated on the basis of the costs payable to the client in the proceedings plus an amount calculated with reference to the funder's anticipated expenditure, or a percentage of total recoveries in the action, there is significant flexibility to tailor commercial terms to the circumstances of individual cases.

The new regime remains in its infancy, but appears likely to radically change the position in respect of access to justice for Plaintiffs with limited resources.

Norwich Pharmacal Relief in support of foreign proceedings

Historically, the Cayman Islands courts have always dealt with a large number of cases with a significant cross-border element, perhaps unsurprisingly given the Islands' position as a critical node within the global financial system. From the point of view of the asset recovery lawyer, that translates into a need for effective and timely interim remedies in order to support overseas proceedings, including pursuant to the *Norwich Pharmacal* jurisdiction.

For many years, it was tacitly accepted in the Islands that *Norwich Pharmacal* relief was available in support of overseas proceedings, but the situation was thrown into some doubt by the decision of Flaux J in the English case of *Ramilos Trading v Buyanovsky*, which took the view that the jurisdiction was ousted as a mechanism to provide evidence for foreign proceedings by the existence of the Evidence (Proceedings in Other Jurisdictions) Act 1975, which sets out a mechanism for the obtaining of evidence by way of judicial request.

Ramilos was not appealed, and although a tension existed with some earlier English decisions on the issue, its effect was to throw the law in Cayman into a state of some uncertainty, the 1975 Act having been extended to the Islands by way of Order in Council. The process for obtaining evidence under the 1975 Order could, even charitably, be described as extremely cumbersome, and is a far cry from the agility and flexibility that has characterised the development of *Norwich Pharmacal* over almost 50 years. As such, its usefulness in obtaining information for the time-critical and dynamic claims that characterise the world of fraud and asset recovery litigation is limited in the extreme.

Faced with that challenge, the reaction of the courts of the Cayman Islands has been swift, reassuring, and cognisant of the clear public interest in ensuring that the jurisdiction is not utilised as a safe repository for incriminating information but instead facilitates efforts to recover the proceeds of fraud.

In *ArcelorMittal USA LLC v Essar Steel*, Kawaley J analysed *Ramilos*, but came to the conclusion that the statutory regime under the Evidence Order was not intended to act as a barrier to justice by automatically ousting the equitable *Norwich Pharmacal* jurisdiction "*without regard to whether or not the statutory regime is accessible in practical terms*". Although stopping short of a finding that *Norwich Pharmacal* will always be available, he pragmatically held that the issue could not be reduced to a simple or formulaic question, and could not be answered so inflexibly as to say that the equitable jurisdiction could not be invoked simply because the material was only likely to be used overseas.

The case then went before the Cayman Islands Court of Appeal where the impact of *Ramilos* was further analysed. A strong bench (Goldring P, Rix JA, Martin JA) rejected the broad contention that the existence of the Evidence Order represented an absolute bar to the use of *Norwich Pharmacal* for the purposes of foreign proceedings. Instead, they arrived at the same conclusion as Kawaley J. They drew an important distinction between the fact that the Evidence Order relates to the obtaining of evidence for use in a foreign proceeding, whereas *Norwich Pharmacal* is concerned only with discovery.

The Court of Appeal emphasised that *Norwich Pharmacal* was based upon a duty to provide information about wrongdoing. It also emphasised that there was no obvious reason why that should be confined only to domestic wrongdoing, or indeed why the existence of legislation dealing with the giving of evidence in foreign proceedings should be treated as excluding a remedy designed to enable proceedings to be brought at all. The enactment of section 11A of the Grand Court Law in 2015, which was intended to place on a statutory basis the jurisdiction of the Court to grant interim relief in relation to foreign proceedings, was relied upon not only as a foundation for the exercise of the *Norwich Pharmacal* jurisdiction to assist

proceedings overseas but also a clear indication that the legislature had no intention to exclude the availability of such remedies.

As such, it was held that if the Evidence Order excluded *Norwich Pharmacal* at all, it was only in the limited circumstances where proceedings were already on foot, or the applicant had available in the relevant jurisdiction procedures for obtaining pre-action disclosure or the provision of non-documentary evidence. In the significant majority of cases, *Norwich Pharmacal* relief would, in principle, remain available.

The decisions of the Grand Court and the Court of Appeal in *ArcelorMittal* are clear examples of not only the independence of the Cayman Islands courts, but also a sensitivity to the importance of disclosure remedies in offshore jurisdictions as a tool to combat abuse. The resolution of the uncertainties temporarily created by *Ramilos* should afford comfort to practitioners that *Norwich Pharmacal*, as a key element of the anti-fraud toolkit, remains un-dulled.

Discovering a fraud - a race against the clock

Limitation periods exist for good reason. Memories fade, witnesses disappear, and parties need certainty. In most cases it is straightforward to calculate the relevant period with reference to established statutory provisions, and the Cayman Islands is no different in that respect. Yet, these rules can pose problems in fraud cases where typically wrongdoing will be deliberately concealed for as long as possible. The issue that arises is establishing the point in time at which enough has been discovered about the fraud so as to start the clock running.

This was one of the key issues considered by the Grand Court of the Cayman Islands in the recent case of *Ritchie Capital Management LLC et al v. (1) Lancelot Investors Fund Ltd and (2) General Electric Company (Parker J)*, which was delivered on 15 December 2020.

Ritchie is a group of funds and investment managers which claims to have lost in excess of US\$200 million as a consequence of the infamous Petters Group Ponzi scheme. Claims were brought in Cayman alleging deceit and unlawful means conspiracy against the feeder fund and lender to the Petters Group. Proceedings were served in mid-2019, and an application was subsequently brought seeking to set aside permission to serve out of the jurisdiction, the principal argument being that the claims were statute barred as it was said that Ritchie knew all it needed to know to bring the claims as long ago as 2009.

In line with many other common law jurisdictions, the Limitation Act provides that where an action is based on the fraud of the defendant, the period of limitation does not begin to run until the plaintiff has discovered, or could with reasonable

diligence have discovered, the fraud. The justification for this extension is clear from a public policy perspective, but whilst it is usually possible to say with reasonable certainty when a fraud was in fact discovered, it is an altogether greater challenge to identify whether there was an earlier point in time where it might possibly have been uncovered.

Parker J adopted the view that the test should be applied in a broad and common sense way, and determined that discovery of facts which would complete the plaintiff's ability to plead the case was the most important factor, with reference to whether there are any facts without which the claim could not be pleaded. However, "common sense" tests tend to import a significant degree of uncertainty, and the situation is more complex in cases of alleged fraud given the ethical considerations in pleading such a claim. A barely arguable case can fall into a grey area, with significant ramifications where the Court takes a different view from counsel as to on which side of the line it falls.

In the case of undiscovered fraud, the court held that what was relevant was not in fact whether the plaintiff 'ought to have' or 'should have' discovered the fraud or concealment, but rather whether with reasonable diligence the plaintiff *could* have done so. This meant that there must first be something which objectively put the plaintiff on notice. If on notice, then comes the question of reasonable diligence, particularly if the plaintiff does not have access to the necessary resources to further investigate the fraud. Parker J accepted that diligence is not an absolute standard and depends on the circumstances, but there must be an assumption that the plaintiff desires to discover whether or not it has been a victim of fraud, and accordingly will take steps to investigate it.

In the instant case, the Petters fraud was widely publicised in 2008, and Ritchie had in fact commenced proceedings against Mr Petters that year. As such, it was apparent that by that stage that Ritchie not only knew that something had gone seriously wrong, but had already starting investigating and bringing actions based on the fraud. Furthermore, Ritchie had also been aware of SEC proceedings against the feeder fund, and had submitted a proof of debt in its bankruptcy in 2013 containing similar allegations to those now made in Cayman, based upon documents obtained in 2009.

In those circumstances, it was considered that Ritchie not only had enough information to be on notice to investigate, but actually had enough information to have discovered at least certain core elements of the fraud from 2009. Although they were not aware of every facet or detail, and further facts might be required to bolster the case, they nevertheless had sufficient information to plead a claim that would survive a strike out application. As such, time began to run in 2009 and the claim was now statute barred.

Conclusion

The decision provides some helpful detail on the process of reasoning applied by the Court in determining questions of this nature, although the answer in any given case remains fiercely fact sensitive. It however acts as a reminder that, when it comes to limitation periods, time waits for no man, even the victims of fraud.

About the Authors



Colette Wilkins QC 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. Colette was appointed to the rank of Queen's Counsel in 2021 following the recommendation of the Cayman Islands' judiciary to the Foreign & Commonwealth office.

Contact Colette Wilkins QC: T. +1 345 914 4215; colette.wilkins@walkersglobal.com

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.

Contact Nick Dunne: T +1 345 814 4548; E. Nick.Dunne@walkersglobal.com



Andrew Gibson is a Senior Counsel in the Insolvency & Dispute Resolution Group at Walkers' Cayman Islands office and member of the Global Arbitration and Global Insurance & Reinsurance practice groups. He has a particular interest in high value asset recovery and crypto-related dispute resolution.

Andrew has a broad practice in commercial litigation, arbitration and ADR, specialising in fraud, asset recovery, contentious insolvency, insurance, professional negligence, real estate and construction disputes. He regularly appears before the Grand Court's specialist Financial Services Division, and has been involved in many high-profile disputes including AHAB v SICL & Others (the most significant fraud trial in terms of value and length ever to be heard in the Cayman Islands).

Andrew played a central role in the electronic discovery process, in which millions of documents in a multitude of languages were critically analysed across 8 countries - the largest ever document review to be managed from the Cayman Islands. Andrew was also involved in the multi-jurisdictional high profile corruption proceedings of Republic of Djibouti & Others v Abdourahman Boreh & Others.

Andrew is an arbitration specialist, advising on all matters relating to arbitration in the Cayman Islands, and has experience of working under a variety of institutional rules, and is also an accredited civil/commercial mediator.

Contact Andrew Gibson: T +1 345 814 4573; E andrew.gibson@walkersglobal.com

Offshore - Decline or Thrive? Can the BVI survive in a world of international minimum level tax treaties and data hacks and leaks?

Shaun Reardon-John

Introduction

The offshore world is generally derided by the international press as a sunny place filled with shady people. It is easy to find stories depicting offshore territories such as the British Virgin Islands (BVI) as small, sparsely populated islands where thousands of companies are incorporated but none do business locally, all with the sinister undertone of money laundering.

This article will summarise some of the steps taken by the BVI in recent years to make information about its financial services sector more accurate and transparent. Many of the legislative initiatives are worthy of an article of their own and as a firm we would be pleased to discuss their impact with any readers who have an interest in how they affect their company or cases.

Recent Developments

Some recent events have provided ammunition to those seeking to demonise the offshore industry. Leaks such as the Panama, Paradise and Pandora Papers - reported by the International Consortium of Investigative Journalists (ICIJ) and its partner media organisations - were exploited for salacious effect, designed to infuriate taxpayers in onshore jurisdictions¹.

The reality was that only a small percentage of the companies disclosed were involved in nefarious actions. Whether the exposure of the few to the detriment of the majority's right to privacy is appropriate is a thorny issue. The focus of the vast majority of companies in these various leaks was legitimate tax "avoidance",

¹ *The Guardian* - Lewis Hamilton avoided taxes on £16.5m jet using Isle of Man scheme (2017)
<https://www.theguardian.com/news/2017/nov/06/lewis-hamilton-avoided-taxes-jet-isle-of-man-scheme-paradise-papers>

something that is not illegal and allowed by ‘onshore’ governments across the world (if governments wished to prevent such avoidance and make it illegal - i.e. tax evasion - they could and should change their laws)².

These offshore misconceptions were illustrated during a panel discussion between our managing partner, Martin Kenney, and the veteran Labour Party MP, Margaret Hodge, during a webinar organised by Offshore Alert in late 2020. Ms Hodge is a strong advocate for offshore reform and one of the principle architects of the public register amendment to the UK Sanctions and Anti-Money Laundering Act. It was startling that despite Ms Hodge’s position as an influential member of the UK parliament, she demonstrated little detailed knowledge about the workings of the BVI financial systems as the debate progressed despite attacking the BVI several times.³

In contrast, it would be interesting to compare the number of genuine tax evasions found in the most recent leaks (the Pandora Papers) against, for instance, the number of frauds committed against the various UK government’s bailout and bounceback schemes during the Covid pandemic⁴. Both show that no system is perfect, but should the UK governments efforts be demonised because of the few in the way the offshore industry has been? That is before we turn to the almost non-existent verification checks of reported identities of Ultimate Beneficial Owners (UBOs) of companies in the UK (something that is thankfully being promised reform).

Outside of the financial services sector, the BVI government has been the subject of an independent commission of inquiry (COI) established in January 2021 by the outgoing BVI Governor, Augustus Jaspert and headed by Sir Gary Hickenbottom. The Commission is not investigating the financial services sector or the Court system in the BVI but, rather “whether there is evidence of corruption, abuse of office or other serious dishonesty that has taken place in public office in recent years, and if so what conditions allowed this to happen.” The narrative promoted by sectors of the press has been that the inquiry into these public officers cannot be distinguished from that of a “shady” financial system (despite efforts to ensure the inquiry’s purpose is clear). Sometimes the truth is simply not as scintillating as a good story.

In addition to the passing events that have affected the BVI, the Territory has also brought into force a steady stream of legislative amendments to combat money

² BBC - Paradise Papers: Everything you need to know about the leak (2017) - <https://www.bbc.co.uk/news/world-41880153>

³ <https://www.youtube.com/watch?v=bH7yaMqgnjl> - see from 32 minutes in. Amazingly, Ms. Hodge felt “confidentiality” and “secret” were the “same thing.” This is clearly incorrect, for instance, if applied to a person’s medical records or bank records.

⁴ <https://www.bbc.co.uk/news/business-59761294>

laundering. Some of these have been voluntary, others forced in order to avoid the Territory being blacklisted by larger states.

Within the European Union's (EU) own borders, there are still member states failing to implement anti-money laundering (AML) legislation that was supposed to take effect in October 2016.⁵ While reviewing the steps taken by the BVI in this article, it is worth comparing the BVI's willingness to act to those "onshore offshore" jurisdictions that appear to be dragging their feet when it comes to AML compliance. This appears to be a classic "do as I say, not as I do" tactic.

Legislative and regulatory steps taken by the BVI to address money laundering risks

As far back as 1997, the BVI introduced the Proceeds of Criminal Conduct Act (PCCA) which provided the core primary legislation to combat money laundering. The PCCA was substantially amended in 2008 by the Proceeds of Criminal Conduct (Amendment) Act 2008 and, more recently, by the Proceeds of Criminal Conduct (Amendments) Act 2021.

As part of the BVI's ongoing steps to ensure reforms keep pace with the risk of abuse the BVI market faces, these amendments have provided steps to modernise the BVI's primary legislation on matters relating to money laundering. This was part of a number of legislative initiatives in 2021, which included the the Proliferation Financing (Prohibition) Act 2021, the Drug Trafficking Offences (Amendment) Act 2021, the Criminal Code (Amendment) Act 2021, the Economic Substance (Companies and Limited Partnerships) (Amendment) Act 2021 and the Beneficial Ownership Secure Search System (Amendment) Act 2021. The aim of the BVI government is clearly to ensure the Territory's legislation keeps pace with new financial risks the world faces.

The PCCA spawned the Anti-Money Laundering Regulations which ensure that regulated persons carrying on regulated businesses in the BVI are required to keep "know your client" (KYC) information about those they do business with. This duty to keep transaction records and ensure there are internal reporting procedures places a duty on financial services businesses in the BVI, who are overseen by the Financial Services Commission (FSC) and the Financial Investigation Agency.

These bodies are charged with receiving suspicious activity reports. In addition to Regulations, the FSC continues to issue Codes of Practice for various sections of the financial services sector. Given the BVI's small size and focus on its financial services

⁵ International Investment (2021) - EU warns Luxembourg with daily penalty threat over AML rules
<https://www.internationalinvestment.net/news/4032879/eu-warns-luxembourg-daily-penalty-threat-aml-rules>

sector as a core pillar of the economy, it appears the Territory is more ready and able to act than many larger countries.

In 2017 the BVI introduced what many consider to be the most significant legislative evidence of its intention to weed out money laundering and tax evasion: the Beneficial Ownership Secure Search System Act (the BOSS Act) which, subject to specific exceptions, applies to all corporate and legal entities incorporated in the jurisdiction.

While the information held on the system has expanded over time to incorporate the requirements of the Economic Substance (Companies and Limited Partnerships) Act 2018, the initial aim was to request, verify and capture the true beneficial ownership details of BVI entities on an annual basis. If sufficient information is not provided, the registered agent will likely resign and the entity will not be able to find a new registered agent until sufficient information is provided.

The system was introduced to facilitate the sharing of beneficial ownership information with specific authorities in order to combat money laundering and tax evasion. There is a continuing duty on a BVI company to keep this information up-to-date, with various levels of fines for infringement by the company and those involved in its administration. The wide definition of a beneficial owner has been key to the legislation's success, capturing those who would otherwise slip through the net using loopholes and includes:

- a. Persons who directly or indirectly own 25% of more of the shares or voting rights
- b. Persons who exercise control over another legal entity that owns the BVI company
- c. Any control via a legal arrangement, e.g. a nominee, so that the legislation can look behind those who claim to control the shares of a BVI company.

The importance of the BOSS system is twofold. Firstly, it allows international agencies to verify the information they have been provided in order to combat money laundering and tax evasion, thus weeding out those who provide inaccurate information to different jurisdictions. Secondly, and crucially, is the accuracy of the information. Registered Agents seek to verify the UBO data during the incorporation process and have processes for regular review by requesting, with appropriate evidence, annual information from the entity to verify there has been no changes to the UBO(s). By comparison to Companies House in the UK, where little or no verification of beneficial ownership information is undertaken at the incorporation stage (though this will hopefully improve due to promised reforms to the system), it is a gold standard system. Similarly, places such as Delaware in the USA do not hold beneficial ownership information: though this too, in some circumstances, should

change due to the introduction of the US Corporate Transparency Act enacted in 2021. Those tracing assets will know that the accuracy of information provided to third parties is key to our work. At the moment it is difficult to see how developed nations can criticise the BVI in this respect, yet they continue to do so.

How the BOSS Act has changed things

Since the BOSS system was introduced, the BVI has utilised the new process as part of its economic substance reporting obligations. In late 2018, the BVI passed the Economic Substance (Companies and Limited Partnerships) Act 2018, which came into force on 1 January 2019. This legislation was in response to EU and Organisation for Economic Co-operation and Development (OCED) pressures, and to similar legislation brought into force in a number of offshore jurisdictions.

In summary, the law created an obligation on certain corporations carrying out relevant activities to evidence that they had an adequate economic presence in the BVI if they claimed to be tax resident here. In practice, this has meant they have needed to show that the relevant activities are directed and managed from the BVI with the associated expenditure you would expect to see from such an entity. If an entity carrying out a relevant activity claims to be tax resident outside the BVI, then documents supporting this claim have to be filed with the BVI International Tax Authority to be assessed whether the entity is exempt from the reporting requirements in the BVI.

These economic substance reports are provided to the company's registered agent and then uploaded into the BOSS system. Because the information needs to be provided annually to the registered agent, it allows a fuller picture of the business to develop over the years, which also helps the registered agent identify any sudden changes that may be cause for concern.

Some have criticised how few requests are made to the BVI authorities to access the information held on the BOSS system. However, this is not a BVI problem but more a sign of the lack of resources available to those who can access it. This begs a question: even if more information is discoverable, will it ever be reviewed? The recent FinCEN leak suggests such volumes of data may be impossible to monitor. What is clear is that the BVI is not a place where it is easy to escape attention if law enforcement or governments want to investigate the source of your wealth.

Tax reform challenges

The next obvious challenge for the BVI and other tax neutral jurisdictions will be the G20's International Tax Reform. The BVI was one of 136 countries to sign up to the agreement last year to impose a minimum 15% corporation tax on the largest

multinational companies, so that profits can be taxed where they are earned. As a tax neutral jurisdiction, it is unlikely that profits will be made in the BVI or at such a scale that a company meets the minimum criteria. Is there a reason to be in jurisdictions such as the BVI at all? Time will tell, but I suspect, in reality, the changes will affect only a small percentage of companies (albeit important ones) since it only affects these businesses with global sales above £17 billion and profit margins above 10%.

What will be interesting to see is how, if at all, a global tax levy on certain businesses will sit alongside the so called “Revenue Rule” which applies across many common law jurisdictions, including England and Wales, the USA and the BVI. In essence, this rule says that the courts of one jurisdiction will not enforce the tax and penal laws (and consequential judgments) of another jurisdiction. While this principle has been slowly eroded over the years, its application going forward will be interesting to follow.

However, the BVI is not beyond criticism. While legislative changes have been positive for many years, there is one ongoing - and concerning - set of implications from legislation that was initially passed in the BVI on 19 March 2020. This concerns the Charging Orders Act 2020 which, seemingly, the government believed was in force. The aim of the Act was to expand the authority of the courts to secure and enforce judgments via a charge over certain assets. The BVI’s Attorney General at the time the Bill was debated, Baba Aziz, stated to the BVI House of Assembly the aim of the legislation:

*“Mr. Speaker, some judgment debtors seek to avoid the enforcement of judgments of the High Court. This Bill is intended to confer jurisdiction on the court to make orders imposing a charge on assets which are **directly or indirectly owned or controlled by a judgment debtor**. This includes where assets or shares are held in layered corporate structures which are ultimately beneficially owned by a debtor. The enactment of this Bill will demonstrate that the Territory is not a haven for recalcitrant debtors and those who would seek to evade justice by means of in part the use of asset protection structures.”*

However, on discovering the Act was not in force, certain sections of the BVI financial services sector sought to lobby for amendments to water down its effectiveness. This has left the BVI government at a crossroads. Does it proceed, as it intended, with a strong piece of legislation aimed at preventing debtors using corporate structures to evade their liabilities, or does it bow down to sections of

dissent within the financial services sector who would seek to protect the interests of these “*recalcitrant debtors*”? At present, no definitive decision has been made.

Can the BVI continue to benefit from its status as an offshore territory?

Financial services are a central pillar to the BVI economy. At its most basic level, the registered agents charge fees for incorporating and maintaining the BVI companies they service. However, the effect of the offshore industry goes deeper for all residents. As a consequence of the companies incorporated there, there is a thriving legal industry, supported by a Commercial Court where the ultimate appellate court is Her Majesty’s Privy Council. This ultimate appellate court is key for many businesses when they incorporate in the BVI.

Then there are the direct benefits to local businesses and landlords from those who purchase services, products or rent accommodation on the island. Should the financial services industry be affected by the ongoing attack on its shores, the consequences for the local population may be devastating. With Covid-19 having decimated the other pillar - tourism - the financial services sector has kept many BVI islanders afloat during the past two years.

A recent report noted that new BVI company incorporations have been in a steady, slow decline for many years⁶. However, the same report says that the lifespan of BVI companies is increasing. This suggests that recent legislative initiatives to remove unscrupulous persons who have abused the incorporation system (such as the requirement to verify the ultimate beneficial owner of a BVI company) is working and that the BVI is moving to a more stable lifespan for incorporations.

What most do not appreciate is that the BVI and other offshore jurisdictions provide companies with the possibility to enter into joint ventures in a tax neutral environment. Such a tax neutral location, coupled with an arbitration centre and a commercial court where the final appellate court is the UK Privy Council, is important. This is especially so for cross-border fledging business which may not initially turn a profit. Once a profit is made, being based in a zero or low tax jurisdiction will mean those losses can be recovered more quickly, keeping the costs of goods down and allowing more profits to be reinvested for further growth. This results in more employment and expenditure and therefore local tax receipts in the countries where the businesses operate - via, for instance, income tax and national insurance contributions in the UK.

⁶ BVI Beacon (2020) - SPECIAL REPORT: Incorporations still falling after 20-year lows in 2019
<https://www.bvibeacon.com/incorporations-still-falling-after-20-year-lows-in-2019/>

There is no doubt that inequality exists in the world. There are leaders of multinational (or even some smaller) companies who seem to leave their conscience at the door when awarding themselves obscene pay, regardless of their enterprises' performance. Increasing tax on corporations is not going to reduce this inequality. Those who lack the moral compass to pay their staff properly, while hoarding profits, may simply increase the prices of products or reduce staff benefits to cover the additional costs. We are not talking about a BVI problem or issue here: this is a worldwide problem. Attacking the BVI, or other offshore jurisdictions, will not change this inequality; neither will increased taxation.

It is likely that the BVI will continue to be an important player in the world's economy. It has proven in recent years that it has the ability to adapt and overcome the hurdles in its way. Asia, South America and now Africa are real generators of financial services work for the BVI. Notwithstanding that, it appears unlikely the BVI will see a sudden increase in incorporations against the long term trend of decline. However, if the life of the average BVI company continues to increase as more multinationals take advantage of its place as a tax neutral jurisdiction (which will remain unaffected by the recent G20 agreement for most businesses), then this increase in quality over quantity should be applauded.

About the Author

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



Shaun's practice also involves commercial arbitration proceedings. He is an advocate of utilising mediation at an early stage of proceedings, having achieved seven figure settlements on behalf of his clients. Having initially joined Martin Kenney & Co. in the BVI in 2012, in August 2019, Shaun became a consultant solicitor for the firm from his base in England, where he continues to work for clients on offshore commercial disputes.

Contact Shaun Reardon-John: T. +1 (284) 494 2444; E. sreardonjohn@mksolicitors.com

Beneficial Ownership Registers Offshore: An Update

Dr Dominic Thomas-James

Background

Over the past few years, we have seen seismic data-leaks exposing economic crime and the offshore world. These have typically been the work of the ICIJ, with the latest taking the name “Pandora papers”. They claim to have unearthed “offshore dealings of 35 current and former world leaders and more than 300 other current and former public officials and politicians around the world”.¹ The ICIJ advances that despite decades of legislative and policy developments in the areas of anti-money laundering and tax, the offshore system continues to “thrive” and the leak is labelled as the largest in the ICIJ’s history, including some “2.94 terabytes of confidential information”.² Such leaks are nothing new, with similar recent instances including the Bahamas leaks in 2016, the Panama papers in 2016, the Paradise papers in 2017, and the FinCEN files in 2020.

The backdrop to these, and similar, leaks is an interesting and complex landscape. We see growing dissatisfaction towards so-called tax havens and the individuals and corporations which utilise them, as well as professional enablers that facilitate and sustain their functioning. Similarly, we see unrelenting momentum in the international community to enhancing global standards in the areas of economic crime and financial regulation - particularly, of recent, in the area of beneficial ownership information transparency.

These inarguably powerful data-breaches have become commonplace and legitimised by governments tasked with legislative reform. The clearest example of this was the passage of the public register provision of the Sanctions and Anti-Money Laundering Act in the UK in 2018 (‘the 2018 Act’): the so-called “Hodge-Mitchell amendment”. This provision created a legislative ultimatum directed at British Overseas Territories that operate financial centres - many of which had been named in various publications emanating from the Panama and Paradise papers. Of the 14 British Overseas Territories in total, some 7 have diversified their economies through the provision of financial and business services, and many are well-known such as

¹ See: ICIJ (3.10.21) ‘Offshore havens and hidden riches of world leaders and billionaires exposed in unprecedented leak’, available at: <https://www.icij.org/investigations/pandora-papers/global-investigation-tax-havens-offshore/> (accessed 10.1.22).

² Ibid, Key Findings, available at: <https://www.icij.org/investigations/pandora-papers/> (accessed 10.1.22).

the Cayman Islands, the British Virgin Islands ('BVI') and Bermuda. Section 51 of the 2018 Act requires them to implement public registers of beneficial ownership (originally with a 2020 deadline, later extended to 2023) or else have them imposed via Order in Council. The manner in which this non-optional reform came to pass demonstrates clearly the weight and influence that Parliamentarians have taken from some of the aforementioned data-breaches. A cursory look at Hansard from the 1 May 2018 debate on the Bill clearly shows the conviction with which British lawmakers viewed the revelations from the Panama and Paradise papers, and the frequency with which these leaks were mentioned in support of the motion.

International Momentum and the Offshore Landscape

Dealing first with the position in the Overseas Territories, who have until 2023 to make their registers public. Following a period of initial tension, with some Territory leaders referring to the non-optional nature of the provision as a “regressive colonial mindset”,³ the Overseas Territories have committed to implementing public registers. Some, like the BVI, made commitments on the basis that public registers become a global standard.⁴ Interestingly, the Crown Dependencies - Jersey, Guernsey and the Isle of Man - committed to the same path, despite the Act not applying to them. However, as indicated, the difference between many territories' stages of legal development demonstrates the problem in legislating in a one-size-fits-all manner. Further, announcing that countries, which are perceived negatively by the international community, are to have 2 or 3 years to make everything public may risk furthering a race-to-the-bottom for suspect wealth to countries which are darker, less compliant, or even opportunistic in this context.

The issue of corporate beneficial ownership transparency is currently being addressed by the Financial Action Task Force in a consultative attempt to devise a new international standard. The fact remains, however, that despite the well-established nexus between dirty money and the facilitative role of anonymous shell companies,⁵ and the constant data-leaks seeking to expose privacy, the international community is wholly unaligned on an international standard on this. Even among ostensibly similar jurisdictions, there is significant disparity in the way corporate ownership information is collected, stored, published and/or exchanged - including whether it is pay-to-access, closed, accessible to law enforcement, or freely and publicly-accessible. When one delves further into the different

³ See Bermuda Government: 'The British Government v The Bermuda Constitution' (4 May 2018), 3-4, available at: <https://www.gov.bm/articles/british-government-vs-bermuda-constitution> (accessed 15 November 2021).

⁴ Government of the Virgin Islands (22.9.20) 'BVI Premier Reiterates Territory's Commitment to an Appropriate Framework for Publicly Accessible Registers', available at: <https://bvi.gov.vg/media-centre/bvi-premier-reiterates-territory-s-commitment-appropriate-framework-publicly-accessible> (accessed 15 November 2021).

⁵ For comprehensive background on this, see: Findley, M., Nielson, D., and Sharman, J.C. (2014) *Global Shell Games*, Cambridge: CUP.

frameworks, it is plain to see that even the most public and freely-accessible registers carry significant shortcomings - particularly in the area of independent verification.⁶

Some examples that further demonstrate the differences in approach internationally include successive E.U. Anti-Money Laundering Directives. For example, the 4th Directive gave the choice to member states as to whether beneficial ownership registers needed to be public or central (i.e. government-held/exchangeable). By contrast, the 5th Directive removed this choice and stipulated that such information - as far as the E.U. was concerned - must be available to the general public. This certainly aligns with the U.K.'s own public register - the register of persons with significant control. It further resembles the Hodge-Mitchell provision of the 2018 Act - namely that there is an imperative for charities, NGOs and the media to have access and be able to scrutinise such information.⁷ Interestingly, the U.S. is a notable absentee of public registers at the point of writing, having only legislated in 2021 to create a central (rather than public) register of beneficial ownership. Of course, this is impacted by the nuance between the State and Federal systems.

Data-leaks as a benchmark

While it is difficult to argue against some of the very serious revelations in some of the aforementioned data-breaches,⁸ one has to consider whether these publications provide compelling justification for reform in this area. For those of us in the financial crime and asset recovery world, the bulk of the revelations were, on the face of them, perhaps relatively unsurprising. Such a view may have even been further exacerbated by the fact that many of the revelations and media coverage pertained to legally permissible conduct,⁹ such as fiscal planning, estate structuring or simply the fact of having investments in a so-called offshore jurisdiction; regardless of whether said investment was actually disclosed and tax paid on any

⁶ I make this point in: Thomas-James, D. (2021) 'Imperfectly perfect, and other concerns about public registers', *Company Lawyer*, Sweet and Maxwell, 42(12), 402-404.

⁷ See Rt. Hon. Andrew Mitchell MP, HC Deb (1.5.18) Vol 640, Col 203.

⁸ See ICIJ website for key findings, above n2. Other overviews of the data-leaks include those reported in the media, such as: BBC (5.10.21) 'Pandora Papers: A simple guide to the Pandora Papers leak', available at: <https://www.bbc.co.uk/news/world-58780561> (accessed 11.1.22); BBC (10.11.17) 'Paradise Papers; Everything you need to know about the leak', available at: <https://www.bbc.co.uk/news/world-41880153> (accessed 20.1.22); and BBC (6.4.16) 'Panama Papers Q&A: What is the scandal about?', available at: <https://www.bbc.co.uk/news/world-41880153> (accessed 11.1.22).

⁹ For example, the Pandora papers purported to show that Tony and Cherie Blair (the former UK Prime Minister and his wife) had saved on stamp duty by purchasing commercial real estate through a legal entity, see: BBC (3.10.21) 'Pandora Papers: Blairs saved £312,000 stamp duty in property deal', available at: <https://www.bbc.co.uk/news/uk-58780559> (accessed 11.1.22). Or, following the Panama papers, the then UK Prime Minister David Cameron admitted to having owned shares in an offshore fund, but sold them before becoming Prime Minister, see: BBC (7.4.16) 'David Cameron had stake in father's offshore fund', available at: <https://www.bbc.co.uk/news/uk-politics-35992167> (accessed 10.1.22).

profits. Even the ICIJ themselves require you to agree to a disclaimer prior to accessing the data-bases, acknowledging that:

“there are legitimate uses for offshore companies and trusts [and] the inclusion of a person or entity in the ICIJ Offshore Leaks Database is not intended to suggest or imply that they have engaged in illegal or improper conduct”.

In terms of assessing what the leaks achieved, at the micro-level the publications clearly opened up investigative lines of inquiry and resulted in numerous instances of exposure and consequent action, broadly-defined. Second, on a more macro-level, the publications did two things. They clearly raised awareness of the offshore world. Yet, importantly, they also created what were, effectively, publicly-accessible databases of company information. This is where recent reforms, such as provisions in the 2018 Act, start to bear greater context. While the information from various leaks paints offshore financial centres, unsurprisingly, in a negative light - a deeper look at the data demonstrates considerable differences in how frequently, or otherwise, some offshore jurisdictions were named in various leaks. This indicates contrast between certain offshore centres in terms of their marketplaces and reliance on incorporation and other corporate services in the given contexts. For example, the Panama papers data indicated that some 3,253 Anguilla-incorporated companies were named, yet sizable number were not active at the point of publication, with some 1,868 active. Elsewhere, in the Paradise papers data, some 9,450 Bermuda-registered entities were mentioned, although, some 6,059 had already been closed. Interestingly, Bermuda was not mentioned in the Panama papers. Elsewhere, some 26 Turks and Caicos-registered entities were named, yet only 2 were active at point of publication.

What is particularly important is the effect such data-leaks have on law in our field. The issue turns on the ability or otherwise to scrutinise and, most importantly, the utility of the information under scrutiny. In some instances in the Panama and Paradise papers, data was old, inaccurate or incomplete and therefore of limited utility. The response, however, was undoubtedly forceful, particularly in relation to British Overseas Territories, specifically: create a public register to stop this kind of thing, or else be compelled to. As one of the architects of the Act, the Rt. Hon. Andrew Mitchell MP averred:

*“closed registers might well allow access to law and order agencies, but that is not enough - they do not allow the same level of scrutiny as the Panama and Paradise papers do”.*¹⁰

It all sounds difficult to argue against - particularly when framed in the context of successive data-breaches, and in a world where we are constantly ceding levels of

¹⁰ HC Deb (1.5.18) Vol 640, Col 203.

privacy in favour of increased convenience. However, when legislators and policymakers are tasked with reforming the law, there must be a moderate chance that a new or amended framework will improve upon the old one. The UK public register, as an example of a world-leading framework, has seen considerable issues,¹¹ particularly vis independent verification. Indeed, Section 51 of the 2018 Act explicitly stresses that:

“[...] the Secretary of State must provide all reasonable assistance to the governments of the British Overseas Territories to enable each of those governments to establish a publicly accessible register of the beneficial ownership of companies registered in each government’s jurisdiction”.

Some Overseas Territories, such as Bermuda, have collected beneficial ownership information for decades and have executed numerous information exchange mechanisms. Given the substantive nature of Bermuda’s financial sector, particularly with its re-insurance market and the business infrastructure built around this, moving from a central register to a public one may well be straightforward to achieve, even without technical assistance. However, for others without the same degree of resources, or levels of legal development, absent meaningful technical assistance, it is difficult to see how effective imposing a system which is so far removed from the current system will be in such a short timeframe. A good example is Anguilla, whose constitution is in desperate need of reform, and who have yet to operate a functioning central register, despite committing to “going public”.

Despite a seemingly global push, it is too early to ascertain whether public registers are the right answer relative to the thing(s) they are trying to achieve. For example, absent effective, independent verification of information submitted to the register, the use of that information from a scrutiny perspective is questionable. As simple as the idea of “going public” sounds, there has been little empirical work considering the effectiveness of public registers versus effective central registers. Effective central registers essentially meet the substance of the FATF Recommendations 24 and 25 on beneficial ownership (i.e. information which is accessible by competent authorities in a timely fashion) and would include mandatory identification verification for officers, agents and ultimate beneficial owners.

It seems as though the architects of the public register provisions of the 2018 Act concede that central registers do work in terms of providing access to law and order agencies. This perhaps erodes the popular conceptions about ‘secret’ registers. If something is accessible to law enforcement, then it is hardly secret from the

¹¹ As background, see: RUSI (29.9.20) ‘Clamping the Wheel of the Money Launderers’ ‘Vehicle of Choice’: Reform of the UK Company Registry’, available at: <https://rusi.org/explore-our-research/publications/commentary/clamping-wheel-money-launderers-vehicle-choice-reform-uk-company-registry> (accessed 10 January 2022); and Global Witness and Open Ownership (2017) ‘Learning the Lessons from the UK’s public beneficial ownership register’, available at: <https://www.globalwitness.org/en/blog/10-lessons-uks-public-register-real-owners-companies/> (accessed 10 January 2022).

standpoint of a criminal - if, indeed, deterring criminality is the principal aim of these particular AML/CFT standards.

The legislation's architects wanted to go further - specifically emphasizing that the media, civic society and charities ought to have access in order to engage in scrutiny. The Panama and Paradise papers data do not, on their own, provide a useful comparison as to what a public register may, or may not look like once it is in place. Such are not sufficient evidence upon which to draw concrete benchmark conclusions on the issue. This is because the leaks were fundamentally different to the concept of a public register given that the exposure of the data occurred overnight, without notice and therefore with the element of surprise. The publications made something which was hitherto private, public and there was no "tipping off". The whole basis of stringent anti-tipping off laws is to preserve the integrity of investigations without the suspect being able to dissipate assets and frustrate legal processes. In the case of the leaks, many named in the media were caught out because they were unaware it was going to happen. In other words, they had a legitimate expectation of privacy and confidentiality prior to the leak. To say that this, i.e. an expectation of privacy, is where the problem lies is powerful but overly simplistic. The reality with such leaks is that many named will be collateral damage, who have not engaged in any type of misconduct or illegality - as the publishers themselves acknowledge.

A concern remains about the extent to which there will be international "buy in" and in a timely fashion. Progress in this regard, even as recently as 2020 in a pre-Covid world, was termed by some watchdog bodies as "patchy".¹² As at publication, according to Open Ownership, some 112 countries are committed to beneficial ownership transparency, with 67 countries reported as partially committed and some 45 being fully committed. Therefore, the issue is far from normative despite being an increasingly visible part of the international AML/CFT framework.

Concluding thoughts

In the field of economic crime, it is difficult to see how anything with the word 'global' in it cannot include the U.S. It is therefore unsurprising that some jurisdictions, such as the BVI, remain somewhat reserved in making a full and unambiguous commitment to implementing public registers. The fact that many UK Overseas Territories operate far less prevalent incorporation markets than BVI, may account for why some in the network have made clearer commitments. Tensions existing in some islands is perhaps understandable, given that many considerably-sized incorporation markets - like some U.S. States exposed in the Pandora papers

¹² 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/5aml-d-patchy-progress/> (accessed 15 November 2021).

for example¹³ - ostensibly do not have to meet the same standards or compliance deadlines as smaller, less influential or equipped jurisdictions like the Overseas Territories.

Finally, there are unresolved issues with relying upon successive offshore data -leaks as sound rationale upon which to build a case for public registers. Public registers may well be an answer, but the picture is far more complex and the journeys that states will have to take in furtherance of their commitments is not insignificant and will not be an overnight concept. Little is said in this discourse of the development challenges that many Overseas Territories, and small island states, face which provides important context in considering their compliance records.

The more often something is said, and the more it is said by those in authority, then the more it is taken as given. It is concerning from a legal point of view that the misappropriation of confidential data can be used as a basis upon which to reform the law, when those behind the dissemination of such data squarely acknowledge that they do not assert that anyone mentioned therein has broken the law.



About the Author

Dr Dominic Thomas-James is a legal academic, international consultant, and barrister. He is the Editor of the Global Annual Report and Consultant to ICC FraudNet. Dominic is a Global Justice Fellow at Yale University, a Research Associate at Fitzwilliam College, Cambridge, and Course Director of the International Development programme at the University of Cambridge Institute of Continuing Education. He earned his Ph.D. and M.Phil. from Queens' College, Cambridge and read law at King's College London. He was Called to the Bar of England and Wales by Inner Temple, and is an accredited commercial mediator. He is author of the book *Offshore Financial Centres and the Law: Suspect Wealth in British Overseas Territories* (2021, Routledge) and his writings are regularly published in journals including as a regular contributor to the *Company Lawyer* (Sweet & Maxwell). Dominic is a senior organiser and participant of the annual Cambridge International Symposium on Economic Crime. He has served as a consultant to various international and inter-governmental bodies, and is often invited to deliver talks and briefings to government and inter-governmental organisations, and at conferences and forums around the world. Dominic is also a practising barrister and Door Tenant at Goldsmith Chambers, London.

Contact Dr Dominic Thomas-James: E. dwrt2@cam.ac.uk

¹³ Washington Post (7.12.21) 'Biden Calls for Sweeping New Push to Expose and Punish Financial Corruption', available at: <https://www.washingtonpost.com/business/2021/12/07/biden-tax-havens-pandora-papers/>, (accessed 10 January 2022).



ICC FraudNet
Global Annual Report 2022

PART FOUR
CYBERCRIME

Legal Developments in Malaysia on Cyber Fraud and Cryptoassets

Lee Shih and Nathalie Ker

Abstract

In this article, Lee Shih and Nathalie Ker, Partners at Lim Chee Wee Partnership, Kuala Lumpur, discuss the recent developments in Malaysian law in the areas of cyber fraud and cryptoassets. They provide an overview of the first ‘persons unknown’ injunction granted in Malaysia, the first decision recognising Bitcoin as a transferable commodity and the Malaysian securities regulator recognising cryptoassets as securities. They further consider the impact that these developments have on the tools used in fraud litigation, including how cryptoassets may now form part of the target assets under freezing orders and proprietary injunctions.

Introduction

In the past few years, Malaysia has seen quite a few developments in the law regarding cyber fraud and cryptoassets. We will touch on three of these. Firstly, the ‘persons unknown’ injunction in Malaysia. Secondly, the Court’s recognition of Bitcoin as a transferable commodity. Thirdly, Malaysia’s securities regulator recognising cryptoassets as securities.

1. First Persons Unknown Injunction in Malaysia

In December 2020, the Malaysian High Court granted the first-ever injunction against persons unknown. This occurred in the case of *Zschimmer & Schwarz GmbH & Co KG Chemische Fabriken v Persons Unknown & Anor* [2021] 7 MLJ 178 (“*Zschimmer*”). *Zschimmer* involved a case of cross-border push-payment fraud. The Court noted that this was an increasingly common cyber fraud where the victim is tricked over

emails to make a payment for a legitimate transaction into a bank account under the fraudster's control. In *Zschimmer*, the fraudster was an unknown party or parties who had infiltrated the email communications between the plaintiff and its South Korean counterparty. The unknown fraudster deceived the plaintiff into paying monies into a bank account in Malaysia under the fraudster's control. The plaintiff thought it was making a genuine payment to the South Korean counterparty.

Upon discovering the fraud, the plaintiff filed an action against 'persons unknown' and the sole proprietor of the bank account. The Court allowed the remedies of a proprietary injunction and freezing order and substituted service by email and Dropbox against the persons unknown.

The Malaysian Court followed the same approach in the United Kingdom in the cases of *CMOC Sales & Marketing Limited v Persons Unknown and 30 others* [2018] EWHC 2230 (Comm), *World Proteins KFT v Persons Unknown* [2019] EWHC 1146 (QB), and *AA v Persons Unknown* [2020] 4 WLR 35 ("*AA v Persons Unknown*"). *Zschimmer* cited these decisions as examples where the Court had the jurisdiction to grant injunctions against persons unknown.

In today's world, where cyber fraud is increasingly sophisticated, this decision is a relief for victims of fraud. Victims will be able to obtain such remedies even where the defendant is unknown due to, for example, the use of fake email addresses.

Zschimmer is also the first Malaysian decision to allow for a proprietary injunction. The Court granted the proprietary injunction over the monies that had been paid out under a false premise. The Court followed the principles set out in the case of *AA v Persons Unknown* where the English High Court granted a proprietary injunction over Bitcoins which had been wrongly transferred. The Court noted that unlike a freezing injunction, there is no need for the plaintiff to show a risk of dissipation of assets.

The Court in *Zschimmer* also ordered for substituted service by way of email with a link to a Dropbox folder. The Court acknowledged that this would be the most practicable method to bring notice of the proceedings to the persons unknown.

In February 2021, the Court further allowed the plaintiff's application for a Spartacus order against the persons unknown. A Spartacus order is a self-identification order requiring the persons unknown to identify themselves and to provide an address for service. The Court applied the English High Court decision in *PML v Person(s) Unknown* [2018] EWHC 838 (QB), where it was held that the purpose of the self-identification order is to ensure that the plaintiff's remedies are effective in the event of a successful claim.

2. Bitcoin Recognised as a Commodity under the Malaysian Contracts Act

Bitcoin and other cryptoassets are still not considered to be legal tender in Malaysia.¹ Nonetheless, the High Court in the case of *Robert Ong Thien Cheng v Luno Pte Ltd & Anor* [2020] 1 LNS 2194 (“*Luno*”) recognised that Bitcoin was a ‘thing’ or commodity. Therefore, Bitcoin could be returned where paid by mistake under section 73 of the Malaysian Contracts Act 1950 (“the Contracts Act”).

In *Luno*, Luno Pte Ltd operated an online wallet and exchange for cryptocurrencies under the trading name of ‘Luno’. It had mistakenly made a double transfer of 11.3 Bitcoins into Robert Ong’s Bitfinex account. Robert Ong admitted to receiving the additional 11.3 Bitcoins but refused to return these. Luno initiated legal proceedings in the Sessions Court to recover the mistakenly transferred Bitcoins. The trial judge at first instance allowed Luno’s claim and Robert Ong appealed to the High Court.

The crux of the appeal turned on whether the Bitcoins could fall under “*anything delivered, by mistake*” under section 73 of the Contracts Act and thus must be returned to Luno by Robert Ong. Robert Ong contended that Bitcoin only existed in the virtual world and where Bitcoin did not take any physical form and was not tangible. Therefore, Robert Ong contended that Bitcoin could not be “*anything*” under the Contracts Act.

However, the High Court agreed with Luno on the argument that the Bitcoins were a form of ‘commodity’ as real money is used to purchase the cryptoassets. There is value attached to Bitcoin in the same way that value is attached to shares. Thus, the High Court held that Bitcoins could fall under the term “*anything*”. Robert Ong was liable to return the mistakenly transferred Bitcoins.

3. Cryptoassets Recognised as ‘Digital Assets’ by the Malaysian Securities Regulator

Cryptoassets have further been recognised as securities by the Securities Commission Malaysia - Malaysia’s securities regulator. Section 3 of the Malaysian Capital Markets and Services (Prescription of Securities) (Digital Currency and Digital

¹ Bank Negara Malaysia and Securities Commission Malaysia, ‘BNM and SC’s Joint Response on “Policy confusion over cryptocurrencies” (16 December 2020) <www.bnm.gov.my/-/bnm-and-sc-s-joint-response-on-policy-confusion-over-cryptocurrencies-> accessed 13 August 2021.

Token) Order 2019² (“the Digital Currency Order”) (referred to by the Court in *Luno*) sets out the requirements for cryptoassets to be classified as ‘securities’.

In 2020, the Securities Commission Malaysia issued guidelines on cryptoassets. Under the guidelines, cryptoassets or ‘digital assets’ are defined as ‘digital currency’ or ‘digital tokens’.³ Cryptoasset exchanges are regulated as digital asset exchanges under this regime.

As at the date of writing, the Securities Commission Malaysia has approved the trading of five digital tokens in Malaysia, i.e. Bitcoin Cash (BCH), Bitcoin (BTC), Ethereum (ETH), Ripple (XRP) and Litecoin (LTC) through the registered digital asset exchanges.⁴

The recognition of cryptoassets as a ‘digital asset’ by the Securities Commission Malaysia is welcome in a world where these digital assets are more likely to form part of a fraudster’s financial portfolio. These may then form part of the assets under freezing orders, proprietary injunctions and eventual tracing reliefs to be granted by the Courts. This brings Malaysia in line with relevant developments in this field in other jurisdictions, particularly the United Kingdom. In November 2019, the UK Jurisdiction Taskforce published a legal statement stating that cryptoassets are to be treated in principle as property⁵ (“Legal Statement”). The English High Court in *AA v Persons Unknown* referred to and adopted the analysis in the Legal Statement in its decision where it recognised cryptoassets as property.

Conclusion

In conclusion, the Malaysian Courts and legislators have together provided more tools for fraud litigators in Malaysia to combat cyber fraud. The principles set out in the cases examined in this article will no doubt be further fine-tuned by the Courts in the future. Given the volatile nature of cryptoassets, it will be interesting to monitor how the Courts apply freezing orders and proprietary injunctions to these assets in different situations.

² Capital Markets and Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019 (8 January 2019) <www.sc.com.my/api/documentms/download.ashx?id=8c8bc467-c750-466e-9a86-98c12fec4a77> accessed 13 August 2021.

³ Securities Commission Malaysia, Guidelines on Digital Assets (28 October 2020), Chapter 4 <www.sc.com.my/api/documentms/download.ashx?id=aeb10f62-944b-4d83-8aa0-4ed492dc1109> accessed 13 August 2021.

⁴ List of Registered Digital Asset Exchanges (Updated list as of 29 July 2021) <www.sc.com.my/regulation/guidelines/recognizedmarkets/list-of-registered-digital-asset-exchanges>.

⁵ UK Jurisdiction Taskforce, ‘Legal statement on cryptoassets and smart contracts’ (November 2019): https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf accessed 29 October 2021.

About the Authors

Lee Shih is the managing partner of the specialist litigation firm, Lim Chee Wee Partnership. He is a member of the ICC FraudNet. His work focuses on fraud and asset recovery, commercial disputes and contentious restructuring and insolvency. He secured Malaysia's first-ever persons unknown injunction against unknown fraudsters as well as self-identification orders. He is also active in advising on and acting in cryptocurrency-related disputes.



Contact Lee Shih: E. leeshih@lcwpartnership.com



Nathalie Ker is a partner in Lim Chee Wee Partnership. Her fraud and asset recovery practice includes high profile and complex fraud matters involving cross-border elements. She is well-versed in obtaining and executing search orders and freezing orders to secure evidence and assets, discovery orders against banks and other third parties, and other interim orders in aid of effective litigation. Nathalie is a founding committee member of the Thought Leaders 4 NextGen FIRE (Fraud, Insolvency, Recovery, Enforcement) Community.

Contact Nathalie Ker: E. nathalieker@lcwpartnership.com

Cybercrimes in Poland: Latest News

Joanna Bogdańska

Abstract

In this article, Joanna Bogdanska, a Partner at KW Kruk and Partners Law Firm LP, discusses the current state of cybersecurity in Poland, citing statistics and taking into account the changing conditions associated with the ongoing epidemic. It points out the weaknesses of the Polish system as well as the latest ideas to address them.

Setting the Scene: a Horrifying Statistic

According to the statistics of the police, crimes against cyber security shows that in 2020, there were almost 55,000 of them¹. This is an increase in over half the cases from the preceding four years. At the same time, the detection of computer crimes is falling. Frankly, it is dramatically low. For example, in the case of attacks on electronic banking, in 2019 it was less than 10 percent. Statistics also indicate that phishing is still the most common crime, which is also mirrored in our experience in practice. Almost 40% of cases which our law office handles involve phishing.

The sudden increase in crime in this area is obviously related to the circumstances of the Covid-19 pandemic and the transition by many institutions and businesses to remote working, for which they were not prepared. For example, they did not have IT security, and it could be said that employees did not have enough knowledge about the risks and how to mitigate them. The scale of the phenomenon is evidenced by the fact that at the end of 2020, there were over 7,400 domains on the scam warning list of CERT Poland.²

The Role and Response of Poland

¹ The statistics are taken from the explanatory memorandum of the draft law on amending the Law on Police and some other laws in connection with the establishment of the Central Office for Combating Cybercrime, available: <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20210002447>.

² The CERT Polska team operates within the structures of NASK (Research and Academic Computer Network) – a research institute which conducts scientific studies, operates the national .pl domain registry and provides advanced IT services. See: <https://hole.cert.pl/domains/> (Accessed 16 December 2021).

It must be admitted that a significant portion of phishing offenses that are related to the Polish jurisdiction are usually not inspired nor initiated by Polish citizens. Some Polish citizens or entities usually play the role of an intermediary or, to be more precise, a tool in the hands of criminals.

This is firstly due to the relative ease of incorporating companies and opening bank accounts for companies in Poland. A company in Poland may be established online within 3 working days. Such an applicant only needs to have a Polish PESEL number (i.e. a tax ID). Such a number can also be obtained by foreign persons without any major problems, for example by declaring the possibility of paying taxes in Poland. In Poland there is also a flourishing business of selling ready-made companies and the acquisition of a company, also by foreign persons, is not controlled in any way. Having a Polish company and having any person with a Polish tax number setting up an account for the company is just a formality. Until recently it was even possible to do it by proxy, without the need to appear in person.

Another issue is the low success rate in detecting such crimes - although we have had some successes. As those reading will appreciate and understand, time is of the essence in such situations. Unfortunately banks are very slow, if at all, to react to suspicious operations on bank accounts, especially if they are accompanied by a description referring to an agreement or an invoice.

Elsewhere, law enforcement authorities, too, cannot boast of high detection rates. Even if they conduct a perfect investigation, their possibilities and options usually end in Poland. Although legal assistance and cooperation within the European Union takes place with relative ease, when it comes to countries outside the European area it is more difficult to obtain information. A curious case from our practice involved a request for legal assistance addressed to an institution in China, for which consideration has been ongoing for about 3 years now. Polish prosecutors do not have any tools to accelerate the examination of such a request. As such, we are still waiting.

Polish legislators seem to recognize the weakness of our system by creating new institutions and strategy plans, but in practice we do not feel any material changes have been made at present. The latest idea is to create a Central Office for Combating Cybercrime and a Cyber Security Fund within the police structure. The office is to be established on 1 January 2022, and whose personnel will be able to identify threats and support citizens in countering and fighting cybercrimes, including cross-border.

About the Author

Joanna Bogdańska is an Attorney at law, and Partner at KW Kruk and Partners Law Firm, Poland. Joanna provides comprehensive legal advice and represents clients in the field of broadly understood economic crime, corruption and fraud leading to exposing business entities to losses.



Joanna participates in conducting audits, including due diligence of business partners, individual transactions and adopted procedures and solutions in terms of compliance thereof with the law. Additionally, Joanna specializes in transaction advisory, with particular focus on mergers and acquisitions. Advises in complex restructuring projects of companies, including mergers, transformations and divisions.

Contact Joanna Bogdańska: T. +48 601 830 633; E. Joanna.bogdanska@legalkw.pl

A close-up photograph of a Bitcoin coin, showing its intricate circuit-like patterns and the word 'BITCOIN' embossed on its surface. The coin is partially obscured by a semi-transparent red rectangular overlay that contains the report's title and part of the main heading. The background is dark, making the metallic coin stand out.

ICC FraudNet
Global Annual Report 2022

PART FIVE

VIRTUAL ASSETS

Applying Traditional Asset Recovery Techniques in the New World of Virtual Assets and Cryptocurrency

James A. Pomeroy

Abstract

In this article, James A. Pomeroy, Director, Forensics at Grant Thornton compares historical asset recovery scenarios and techniques with current trends in blockchain-enabled cryptocurrency and other virtual assets. He provides an overview of virtual assets, differentiating between the enabling technology, the assets themselves, and those who would (mis)use the technology to defraud or to conceal misappropriated value. He further discusses, with examples, how lawyers, the judiciary, investigators, and data analysts have adopted historical asset recovery techniques and developed new ones to address the shifting virtual asset cyber-scape.

Introduction

Virtual assets are recorded, stored, and transacted on blockchain technology. To many, the terminology can be overwhelming, and terms for very different aspects of virtual assets and the underlying technology ecosystem are often used, improperly, synonymously. A basic understanding of what blockchain is and how it works is helpful if the asset recovery profession - including lawyers, investigators, data analysts, and even the judiciary - is to keep up with the pace of technology.

Unlike a traditional accounting ledger with a single point of entry, the distributed nature of the blockchain means that multiple, indeed maybe thousands of copies of the ledger are maintained on different network nodes. Each node, or participant, shares in the highly complex calculations that underly the cryptography generating

a ‘hash value’¹ that validates data as it is being added to the database and protects that data from tampering. The entire history of all transactions is maintained on each node. If one node were to vary, the system would easily identify the anomaly. Changes to the history would require the agreement and computing power of the entire network.

Since all transactions and all copies of the database are continuously and automatically agreed to one another each time a record, or ‘block’, is added the data (the balance in a crypto wallet, a non-fungible token (‘NFT’) for a digital work of art, and so on) remains unchangeable, trusted, and secure.

There is an irony in that blockchain - the very technology that enables cryptocurrency, built to assure, or even eliminate the need for trust - has been co-opted by fraudsters and criminals who have breached the trust of their victims.

Trust and Volatility

The current volatility experienced by cryptocurrency markets driven, for example by Tesla tweets, a crackdown in China, and the somewhat bumpy adoption of Bitcoin by El Salvador, might seem to undermine trust in the virtual asset world for everyday investors and speculators. In one day in May 2021, Bitcoin market cap dropped by nearly one third before rallying and settling down by around 12%². We should be clear, however, to differentiate between our trust issues with the technology and virtual assets that rely on it, rather than with the humans who use the technology for dark purposes. While we can trust the technology itself, it is the users, their actions, and the market reactions, of which we must be cautious.

For the corrupt, the fraudsters, and anyone else looking to avoid scrutiny or hide assets, the volatility of cryptocurrency and the perils lurking in the darker corners of the virtual world are simply part of the cost of doing business. The same volatility also draws everyday investors looking to ride the wave but who often fall victim to rapid shifts in value, or to predatory actors.

The increasing prevalence of cryptocurrency and the growing adoption of it and other burgeoning virtual assets has radically changed the playground for those

¹ “Hash values can be thought of as fingerprints for files. The contents of a file are processed through a cryptographic algorithm, and a unique numerical value - the hash value - is produced that identifies the contents of the file. If the contents are modified in any way, the value of the hash will also change significantly. Two algorithms are currently widely used to produce hash values: the MD5 and SHA1 algorithms.” - Author Unknown, *TrendMicro.com*, See: <https://www.trendmicro.com/vinfo/us/security/definition/hash-values> (Accessed 7 October 2021)

² Nathan Reiff, *Investopedia* (16 June 2020), See: <https://www.investopedia.com/articles/investing/052014/why-bitcoins-value-so-volatile.asp> (Accessed 7 October 2021)

looking to hide ill-gotten gains. Part of their acceptance of the volatility associated with this asset class must be attributable to the trade-off of certainty of value for the anonymity (perceived or actual) and the decentralised nature of the underlying blockchain technology.

Fortunately, the technology that works for the fraudsters can also work for those who follow them. This paper will provide an overview of the virtual asset landscape and considerations for asset recovery professionals.

Virtual (Digital) Assets: An Overview

The pace of the discussion surrounding cryptocurrency among asset recovery practitioners has come with the introduction of a whole new vocabulary. This is surely understood differently according to one's degree of exposure and level of experience. It's easy to conflate the concepts and terminology, however, there are a few basic terms that would be worthwhile to recognize as related, but different. In this paper the terms 'virtual assets' and 'digital assets' are used interchangeably.

The Cayman Islands Ministry of Financial Services defines virtual assets quite simply as “a digital representation of value that can be electronically traded and used for investment purposes.”³

In England and Wales, digital or crypto assets have been defined by the UK Financial Conduct Authority as: “cryptographically secured digital representations of value or contractual rights that use some type of distributed ledger technology (DLT) and can be transferred, stored or traded electronically.”⁴

A common type of virtual asset is cryptocurrency, but it is a subset of, rather than a synonym for, virtual assets. Other virtual, or digital, assets may be derivative from one or more cryptocurrencies, or they may not be intended as currencies at all.

A cryptocurrency is a digital, or virtual asset that is created as a currency, a means of storing and transferring value, that is secured by cryptographic calculations. The digital record is maintained on an immutable, decentralized, public or private blockchain network.

³ Ministry of Financial Services, Cayman Islands Government News. See: <https://www.mfs.ky/news/information/faqs-on-virtual-asset-service-providers> (Accessed 7 October 2021)

⁴ Financial Conduct Authority, “Guidance on Cryptoassets - Consultation Paper CP19/3” (January 2019) See: <https://www.fca.org.uk/publication/consultation/cp19-03.pdf> (Accessed 22 October 2021)

An NFT uses cryptography to secure the record of ownership of a digital or even a physical asset⁵. NFTs serve as evidence of provenance and in doing so, may provide some assurance to the owner of their legal right to the asset, however, unlike cryptocurrencies and other digital assets, they do not, in and of themselves, store or transfer value. The value remains with the underlying asset but is bolstered by the NFT. For asset recovery professionals, this may be analogous to how the value of an aircraft engine relies on the existence and validity of the engine's maintenance record documentation. The intrinsic value is in the asset, but there is added value to having a robust record ownership and state of condition. Like cryptocurrency and other digital assets, the NFT's encrypted smart contract is recorded on a decentralized, distributed blockchain ledger.

Unlike government-issued currencies, the value of many cryptocurrencies is a function of its scarcity and the costs of creating new coins whereas others, called "Stablecoins", are a class of cryptocurrency that are purportedly backed by, or tethered to, fiat currency, precious metals, or other commodities. There are ongoing issues with whether Stablecoins are, in fact, "stable".⁶

Virtual assets may operate on their own private blockchain network, or they may use public blockchain technology.

A fulsome discussion of the gamut of virtual assets is beyond the scope of this paper, though it is a worthwhile takeaway to remember that while all cryptocurrencies are virtual assets, not all virtual assets are cryptocurrencies. Consider, for example, security tokens issued as virtual representations of traditional securities, like shares voting rights and dividends, which take advantage of the underlying cryptographic security, transparency, speed, and ease of audit that blockchain technology provides.

What Does it all Mean for Asset Recovery?

Traditional asset recovery strategies and techniques apply to many different situations from the recovery of the proceeds of crime, identifying and realizing the assets of an insolvent estate, civil judgment enforcement, to providing access to justice for victims of fraud. While it may factor into the strategic asset recovery plan, the nature of the loss is not necessarily the headline issue.

⁵ L. DeNicola, "What to know about non-fungible tokens (NFTs)— unique digital assets built on blockchain technology", *Business Insider* (1 September 2021), See: <https://www.businessinsider.com/nft-meaning> (Accessed 7 October 2021)

⁶ Kadhim Shubber, Joshua Oliver and Siddharth Venkataramakrishnan, "*Tether's bitcoin-backed lending clashes with dollar promise*" (19 October 2021), See: <https://www.ft.com/content/0035016c-29ad-4e6f-9163-2a17df490aa5> (Accessed 22 October 2021)

Similarly, in the world of virtual assets, practitioners may encounter situations where cryptocurrency has been integral to the loss, for example, where ransomware payments are made in Bitcoin or an initial coin offering proved to be fraudulent. Equally, the involvement of cryptocurrency can also be merely a by-product of a traditional fraud and can be used to cloak the transfer of value in the ‘grey box’ of the cryptocurrency world.

While it’s true that passing value through cryptocurrency or another virtual asset adds complexity to the asset recovery process, it is also true that traditional investigative, tracing, and legal techniques still apply. What might be new territory for practitioners are the subjects of those traditional orders, or the creativity required to have them apply.

Adapting to the Virtual World

The case of *AA v Persons Unknown who demanded Bitcoin on 10 and 11 October 2019 and others* [2019] EWHC 3556 (Comm.)⁷ is a matter in which ransomware was paid on behalf of an insured cyber insurance policyholder in exchange for the recovery of access to corporate data following a malware attack. Naturally, after paying the Bitcoin ransom and upon regaining access and control over its data, the cyber victim insurer took steps to try and recover the ransom payment and engaged a specialist technology firm to assist. The English Commercial Court was prepared to grant a proprietary injunction in respect of most of the Bitcoin ransom which had been traced to a trading account at a well-known exchange. The case is a signpost to where asset recovery is moving.

Historically, in an analog world, the victim’s response team might have involved asset recovery counsel or engaged investigators to track the perpetrators, and possibly forensic accountants to trace money wired to an offshore account. Time would have been of the essence, but it would have taken time to bring a series of Norwich Pharmacal or 28 USC 1782 applications across multiple jurisdictions, leading to multiple iterations of tracing through bank accounts to unravel the flow of funds.

In *AA vs Persons Unknown*, the court was prepared to grant ancillary disclosure orders against the relevant exchange where the relevant account had been identified using analysis of the blockchain. In other words, the applicant insurer was aided by more modern tools and the adaptation of existing ones to quickly zero in on what had transpired with the ransom payment.

Blockchain technology has the advantage (to investigators and analysts) of transparency, or at least semi-transparency, in that the timing, amount, source, and

⁷ *AA v Persons Unknown who demanded Bitcoin on 10 and 11 October 2019 and others* [2019] EWHC 3556 (Comm.). See: <https://www.bailii.org/ew/cases/EWHC/Comm/2019/3556.html> (Accessed 7 October 2021)

destination of every transaction ever made is publicly available. Transaction details are linked to the participants by a public cryptographic key, generally represented by a unique alphanumeric string.

A public key is just that, *public facing*, which allows parties to send and receive cryptocurrency. The catch, then, is that a private key is required to initiate a transaction and the identity of the holder of those private keys is *not* public. The result is the concept of pseudo-anonymity, or the ‘grey box’.

With sufficient intelligence and through complex data analysis, certain relationships can be identified within the ‘grey box’, and it may be possible to link a public key with other public keys. An analogy might be if one were to visually observe criminal activity taking place on a particular street corner with this activity occurring regularly, week after week. In fact, you might occasionally observe the police intervene to question different parties or make arrests. Such a street corner might eventually garner a reputation for hosting illicit activity, which, from an intelligence perspective, could enable one to deduce that an individual approaching the corner late one evening is quite likely up to no good.

Caution is required, however, in relying on such deductions alone, since traffic past the dark corner does not necessarily denote wrongdoing. In the new and complex virtual world, it would be quite possible for an unsophisticated person who’s simply looking to test the crypto market to find themselves inadvertently drawn into dealing with a bogus exchange. In fact, as in the real world, criminals and fraudsters of all types regularly take advantage of unwitting victims who find themselves alone in the wrong “dark alley”. These considerations are among many that drive the development of extremely complex heuristics models that examine traffic on the blockchain⁸.

In *AA v Persons Unknown*, the specialist blockchain analysis company deployed its investigative analytics model and their experienced analysts produced a roadmap following the ransom payment through the Bitcoin blockchain network. The analysis connected the tainted payment with certain specific public keys that were known to be related to cryptocurrency exchanges and to public keys where value remained.

At that point, the identity of the perpetrators was still unknown, but the intelligence provided a strong foundation upon which the victim’s insurer’s counsel brought an application to the court seeking, among other things, Norwich Pharmacal/Bankers Trust-style relief. The objective was to connect the public keys linked to the ransom payment to the individuals behind those keys in order to bring claims to recover the Bitcoins, or the value of the ransom payment in fiat currency.

⁸ Yhuang Zhang, Jun Wang, and Jie Luo, “Heuristic-Based Address Clustering in Bitcoin”, *IEEE Access* (7 December 2020), See: <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9265226> (Accessed 12 October 2021)

In *AA v Persons Unknown*, the court wrestled with the issue of whether cryptocurrency was in fact property that would be subject to a proprietary injunction.

“Turning then to the relevant principles in relation to the granting of a proprietary injunction, the first and perhaps fundamental question that arises in relation to this claim for a proprietary injunction is whether or not in fact the Bitcoins, which are being held in this account of the second defendant with the third or fourth defendants are property at all. Prima facie there is a difficulty in treating Bitcoins and other crypto currencies as a form of property: they are neither choses in possession nor are they choses in action. They are not choses in possession because they are virtual, they are not tangible, they cannot be possessed. They are not choses in action because they do not embody any right capable of being enforced by action. That produces a difficulty because English law traditionally views property as being of only two kinds, choses in possession and choses in action.”⁹

While the court recognised that it did not in fact constitute law, the court demonstrated pragmatism and agility, finding it relevant to consider analysis provided in a recent (November 2019) “Legal Statement on Crypto assets for Smart contracts” issued by the UK Jurisdictional Task Force and adopted the analysis recognizing crypto currency as property. Ultimately, the court concluded that cryptocurrencies are a form of property capable of being subject to a proprietary injunction:

“In those circumstances and for the reasons I have given, as elaborated upon in the Legal Statement which I gratefully as what I consider to be an accurate statement as to the position under English law, I am satisfied for the purpose of granting an interim injunction in the form of an interim proprietary injunction that crypto currencies are a form of property capable of being the subject of a proprietary injunction.”¹⁰

In addition to a proprietary injunction and orders for service outside the jurisdiction, the insurer’s application originally sought Norwich Pharmacal / Bankers Trust orders to uncover information from the cryptocurrency exchange about the relevant account owned or controlled by the Persons Unknown. During the course of oral argument, the court noted certain complications arising from the multi-jurisdictional structure of the exchange and the location of two corporate entities in the British Virgin Islands (“BVI”).

Given the court’s jurisdictional concerns around the effectiveness of English court ordered Norwich Pharmacal relief against BVI entities, as well as additional

⁹ *AA v Persons Unknown who demanded Bitcoin on 10 and 11 October 2019 and others* [2019] EWHC 3556 (Comm.), paragraph 55

¹⁰ *Ibid.* at para.61

jurisdictional concerns relating to service, the insurer’s counsel sought and obtained the relevant disclosure order as ancillary relief to the proprietary injunction.

Subsequently, in the case of *Ion Science and Duncan John v Persons Unknown, Binance Holdings & Payward Limited (unreported)*, 21 December 2020 (Commercial Court), the English courts have been prepared to make disclosure orders against respondents located outside the jurisdiction pursuant to the Bankers Trust jurisdiction.

Nevertheless, *AA vs Persons Unknown* remains an important benchmark case, not only for the legal conclusion that cryptoassets can constitute property for the purposes of English law but also in demonstrating how the “old world” of asset recovery techniques can be adapted to the “virtual world”.

The Horizon

There are perhaps some obvious applications of traditional legal and asset recovery techniques to the world of virtual assets. For example, targeting exchanges for discovery orders. As the body of case law develops, legal and investigative practitioners, data analysts, and the courts will find more opportunities to use tried and true techniques in new ways.

Exchanges and other intermediaries are becoming richer targets for disclosure orders to access information about the source of funds and the identity, and possibly location, of individuals who control public keys that have been associated with criminal behavior.

There are hundreds or thousands of exchanges across the globe and, with barriers to entry being relatively low, they can appear and disappear very quickly. More reputable ones and those wanting access to high population markets which will require higher levels of know-your-customer (‘KYC’) and anti-money laundering (‘AML’) compliance programs.

As the adoption rate and acceptance of cryptocurrency continues to rise, exchanges that want to reach new customers and offer new services will face increasing demand for enhanced KYC and stricter regulation. This will further open up targets for discovery orders in asset recovery cases.

In the short and medium term, tightening regulatory models around the world may force less reputable or poorly certain capitalised exchanges to cease operations or move further into the fringe of less rigorous regulatory environments, a so-called “race to the bottom”.

Regulatory developments are likely to lead to the more reputable exchanges who are looking to expand their markets and introduce new services to curtail their

expansion. In fact, less than a year after disabling its margin trading product¹¹, Coinbase, one of the world's top spot cryptocurrency exchanges¹², recently deferred its plan to move into digital asset lending, citing pressure from the US Securities and Exchange Commission¹³.

The mainstreaming of regulation in the crypto industry will lead to a wider dichotomy of virtual asset services and providers. Everyday users will be drawn to the “safety” of a regulated industry and users who strongly value their anonymity, especially those involved in nefarious activity, will follow new or existing exchanges to darker corners of the virtual world with less governance and greater risk. It's just the latest spin on an old game.

Conclusion

Whether adopting old tricks or learning new ones, asset recovery practitioners must keep pace with the evolution of virtual asset (and debt) products. Investigators and lawyers are collaborating now and as blockchain analytics and technologies evolve, new strategies are emerging. Moving beyond discussions, use cases are being developed to take advantage of the vast data sets that are available to blockchain analysts. They are proactively monitoring blockchain addresses where value has been traced to ultimately freeze and seize virtual assets before they exit the ‘grey box’, or move sideways to a different box.

As more and more cases play out, the field will inevitably find new ways to take advantage of the attributes and technology that enable the world of virtual assets.

¹¹ Paul Grewal, Chief Legal Officer, *The Coinbase Blog* (24 November 2020) See: <https://blog.coinbase.com/coinbase-pro-disables-margin-trading-42f5862f8a66> (Accessed 8 October 2021)

¹² Coinbase Exchange was ranked number 2 among spot cryptocurrency exchanges according to CoinMarketCap.com rankings, as of 8 October 2021.

¹³ Hannah Murphy and Stefania Palma, *Financial Times* (20 September 2021) See: www.ft.com/content/bd09f8bf-e65b-4870-affe-55b5346af3e1 (Accessed 8 October 2021)

About the Author

James Pomeroy, CPA CA, CFE is Director, Forensics, and heads Grant Thornton's Forensics practice in the BVI, Cayman Islands, and the Eastern Caribbean. He has 26 years of insolvency, audit, forensic accounting, and investigations experience, 21 of those with a Big Four firm. He is a Chartered Professional Accountant, a Fellow of INSOL, and a Certified Fraud Examiner.



James' experience includes cases involving asset tracing and recovery, investigations, cross-border insolvency, political corruption, business intelligence and integrity due diligence, commercial fraud and disputes, and forensic technology. He has experience in matters originating in jurisdictions throughout the offshore financial sector, in the Caribbean region, Latin America, Canada, Switzerland, the US, and Hong Kong.

James has led insolvency-based asset tracing and recovery engagements and investigations in jurisdictions around the world. James is an experienced forensic accountant and asset recovery professional with an appreciation for the nuances of different regions and cultures and how those can impact a case.

Contact James Pomeroy: James.A.Pomeroy@uk.gt.com

To Regulate or Not to Regulate: Law Enforcement, Criminal Cartels and the Legitimation of Cryptocurrency

Kate McMahon

Abstract

In this article, Kate McMahon, founder and Partner at Edmonds Marshall McMahon, examines the complex world of cryptocurrency, and considers some of the ongoing regulatory questions and developments affecting cryptoassets. With reference to recent and high-profile examples, the paper addresses some of the challenges and threats posed by virtual assets.

1. Introduction

In 2008, the elusive Satoshi Nakamoto published the bitcoin white paper (the “White Paper”). Satoshi Nakamoto is the pseudonym used by the person (or indeed persons) who developed bitcoin - the cryptocurrency that is widely considered to be the first of its kind. Although the real-world identity of bitcoin’s creator is unknown, this cryptocurrency has had a meteoric rise. In just over ten years, it has moved from the periphery of markets to become a billion-dollar asset class. On 30 July 2021, bitcoin’s total market capitalisation stood at almost \$750 billion (\$743,949,021,182 to be exact).¹

This ascent is part of a wider trend. Since bitcoin’s birth, a host of imitators (some legitimate, some less so) have entered the cryptocurrency arena. As of 28 July 2021, the total market capitalisation of cryptocurrencies was over \$1 trillion.² Notwithstanding the rapidly developing cryptoasset market, great uncertainty has plagued cryptocurrencies. Investors, lawmakers and regulators around the world have all had trouble classifying this new type of asset (a necessary precursor to

¹“Today’s Cryptocurrency Prices by Market Cap”, *CoinMarketCap*, 30 July 2021, available at: <<https://coinmarketcap.com/>> last accessed 30 July 2021.

² “Global Cryptocurrency Charts”, *CoinMarketCap*, 28 July 2021, available at: <<https://coinmarketcap.com/charts/>> last accessed 28 July 2021.

regulating it). As it stands, therefore, digital assets and their exchanges remain largely unregulated - the new Wild West, as it were.

So, what are cryptocurrencies? The White Paper outlines the principles governing bitcoin and is a sensible place to start. This document describes a cryptographically secured, *“purely peer-to-peer version of electronic cash [which] would allow online payments to be sent directly from one party to another without going through a financial institution”*.³ The White Paper also describes the much-lauded blockchain technology (a system that records transactions in bitcoin). This technology provides *“proof-of-work”*, by recording a *“public history of transactions that quickly becomes computationally impractical for an attacker to change”*.⁴

In addition to transparency, *“strong control of ownership”* is identified as a key principle.⁵ The White Paper explains that cryptocurrencies do not need a bank to carry out transactions between individuals. The nature of the blockchain means that individuals can transact with each other, even if they do not trust each other. It would appear, therefore, that bitcoin was designed to be fundamentally transparent (at least to the holder of bitcoin) and to give individuals financial control.

In order to understand these founding principles, it is essential to look at the historical context. When the White Paper was released, the world was gripped by the 2007 financial crisis, triggered by excessive speculation in financial markets and overzealous lending by banks. Prior to the devastation caused by COVID-19, this was considered by many economists to be the worst economic crisis since the Great Depression.

Although the White Paper does not explicitly say so, bitcoin appears to be a reaction to the 2007 crisis and, more broadly, to the financial world’s reliance on banks that had let ordinary consumers down.⁶ If this analysis is correct (and bitcoin was intended to empower individuals and protect consumers from mainstream banks) it is ironic that commentators are now calling cryptocurrencies the biggest scam in financial history. Top government officials in India have gone so far as to call cryptocurrencies a Ponzi scheme.

2020 and 2021 have been stunning years for cryptocurrency, providing investor returns that appear too good to be true. Even in the midst of the COVID-19 pandemic, bitcoin has soared to new heights. On 26 July 2021 bitcoin traded at just

³ Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System” (2008) available at: <https://www.usssc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf> last accessed 28 July 2021.

⁴ *Ibid.*

⁵ *Ibid.*

⁶ Ollie Leech, “What is the Bitcoin White Paper”, *CoinDesk*, 21 January 2021, available at: <<https://www.coindesk.com/what-is-the-bitcoin-white-paper>> last accessed 30 July 2021.

above \$40,000, and in mid-April bitcoin traded at its all-time high of \$65,000.⁷ Ostensibly, cryptocurrencies have not only lived up to the hype, but they have finally become mainstream. Or have they?

The truth is that bitcoin is affected by chronic volatility. For example, on 20 July 2021, bitcoin's price fell below \$30,000, representing a 50% decline from April. In fact, almost \$90 billion was wiped off the cryptocurrency market in a mere 24 hours.⁸ Cryptocurrency is also fuelling a spectacular growth in cybercrime. Whatever fans may say, cryptocurrency *is* very appealing to criminals because of its anonymity, user control and the speed of transactions - and it is being used to catastrophic effect. By way of example, in April 2019, Mexican police arrested human trafficker Ignacio Santoyo, who allegedly blackmailed and sexually exploited 2,000 women. The longevity of Mr Santoyo's trafficking scheme was facilitated (in part) by bitcoin, which was used to launder his operation's proceeds.⁹ According to Santiago Nieto (head of Mexico's Financial Intelligence Unit), this type of scheme is becoming increasingly common - "*there's a transition to committing crimes in cyberspace, like acquiring cryptocurrencies to launder money... and the pandemic is accelerating it*".¹⁰

And so, a conflict has emerged. On the one hand, cryptocurrency is providing stunning investor returns and offers an exciting new technology. However, the light-touch regulatory approach that has enabled cryptocurrency's rise has clear drawbacks - namely, that pricing is unstable and crypto-networks are being used to commit crimes. All this has raised a simple question for governments around the world - to regulate or not to regulate?

2. The current regulatory landscape

2.1. *The UK*

As it stands, rules and regulations governing cryptocurrencies are sparse. In the UK, there is still no statutory definition of cryptocurrency, nor is there any legislation governing this type of asset directly. There are a number of reasons for this. First,

⁷ Arjun Kharpal and MacKenzie Sigalos, "Bitcoin briefly tops \$40,000 for the first time since June as cryptocurrency rallies after sell-off", *CNBC*, 26 July 2021, available at: <<https://www.cnbc.com/2021/07/26/bitcoin-btc-price-tops-39000-for-the-first-time-in-nearly-6-weeks.html>> last accessed 30 July 2021.

⁸ Arjun Kharpal, "Bitcoin drops back below \$30,000, heads toward new low for the year", *CNBC*, 19 July 2021, available at: <<https://www.cnbc.com/2021/07/20/bitcoin-btc-falls-below-30000-as-cryptocurrency-market-plunges.html>> last accessed 30 July 2021.

⁹ <https://www.reuters.com/article/mexico-bitcoin-idUSL1N2IJ01D>

¹⁰ Diego Oré, "Insight - Latin American crime cartels turn to crypto to clean up their cash", *Reuters*, 8 December 2020, available at: <<https://www.reuters.com/article/mexico-bitcoin-insight-idUSKBN2811KD>> last accessed 30 July 2021.

the sheer speed with which cryptocurrencies infiltrated the global financial system has meant that regulators have not been able to keep pace. Secondly, there has been considerable confusion about what this new kind of asset actually is. Until recently, commentators were unable to agree on whether cryptocurrency is property, a right or something else entirely.

Fortunately, in November 2019, the UK Jurisdiction Taskforce (the “UKJT”), headed by Chancellor of the High Court, Sir Geoffrey Vos, published its Legal Statement on Cryptoassets and Smart Contracts (the “Statement”).¹¹ This provided much-needed clarity on the legal status of cryptocurrency, concluding that it should be treated as property, as it possesses all the necessary “indicia” to qualify as such.¹²

While the Statement was a step in the right direction, there remain difficult questions around what cryptocurrency is, what its benefits are and what a regulatory regime might look like. As the Statement says, it was only intended to address the “*prior issue of common law characterisation*” and, necessarily, it only provided high-level analysis.¹³ In the words of Sir Geoffrey Vos, “*there is no point in introducing regulations until you properly understand the legal status of the asset class that you are regulating*”.¹⁴

While many envisaged the development of a comprehensive regulatory regime, based on the UKJT’s principles, there has been scant progress since the Statement. The UK Government has, however, signalled that regulation is coming down the turnpike. In January 2021, the UK Treasury published a document entitled “*UK regulatory approach to cryptoassets and stablecoins: consultation and a call for evidence*” - a clear precursor to the building of a regulatory framework.¹⁵

¹¹ “Legal Statement on cryptoassets 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 23 July 2021.

¹² The Statement, paragraphs 39 and 40.

¹³ The Statement, paragraph 10.

¹⁴ Sir Geoffrey Vos, “The Launch of the Legal Statement on the Status of Cryptoassets and Smart Contracts”, 18 November 2019, available at:

<https://www.judiciary.uk/wp-content/uploads/2019/11/LegalStatementLaunch.GV_2.pdf> last accessed 23 July 2021.

¹⁵ “UK regulatory approach to cryptoassets and stablecoins: consultation and a call for evidence”, *HM Treasury*, January 2021, available here:

<https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950206/HM_Treasury_Cryptoasset_and_Stablecoin_consultation.pdf> last accessed 26 July 2021.

2.2. The USA

The UK is not the only jurisdiction that has had problems classifying cryptocurrency. In the USA, there has been fierce debate among academics, lawmakers and government officials about whether cryptocurrencies are actually disguised securities, to which securities regulations should apply. In 2018, Gary Gensler - the former Chairman of the U.S. Commodity Futures Trading Commission - argued that Ethereum (the second most established cryptocurrency) is a security, to which securities law should apply.¹⁶ Shortly thereafter, Jay Clayton - the head of the U.S. Securities and Exchange Commission (“SEC”) - contradicted this, asserting that cryptocurrencies are *not* securities and that the SEC would not change securities law to cater for this new asset.

The longstanding definition of security follows the 1946 Supreme Court case *SEC v. W. J. Howey Co.*¹⁷ This case established the ‘Howey Test’, which classifies a security as (1) an investment of money (2) in a common enterprise (3) in which the investor expects profits (4) primarily from others’ efforts.

Applying this test to cryptocurrency, buying bitcoin may be seen as an investment of money and involve the expectation of profits (if a buyer’s intention is to hold the currency). That said, although many people see bitcoin as a speculative instrument, this is not what it was intended to be. Bitcoin was created to be a peer-to-peer payment network, allowing users to buy goods without transacting through a bank. It is also a stretch to argue that a cryptocurrency network is a “common enterprise”, when the intentions of users are so diverse. Similarly, profits made from cryptocurrencies do not accrue from others’ efforts - they depend on market forces, the consumer zeitgeist and a currency’s perceived usefulness.¹⁸

This conclusion - that the cryptocurrencies do not meet the Howey Test - was confirmed by Mr Clayton in an interview with CNBC news. He explained that cryptocurrencies are “*replacements for sovereign currencies... [they] replace the dollar, the euro, the yen with bitcoin. That type of currency is not a security.*” He further explained that the USA has built a \$19 trillion securities market that is the “*envy of the world*”. As such, the SEC would not be doing “*any violence to the*

¹⁶ Annaliese Milano, “Everything Ex-CFTC Chair Gary Gensler Said About Cryptos Being Securities”, *CoinDesk*, 24 April 2018, available at: <<https://www.coindesk.com/ex-cftc-chair-gary-gensler-on-tokens-securities-and-the-sec>> last accessed 28 July 2021.

¹⁷ *SEC v. W. J. Howey Co.*, 328 U.S. 293 (1946).

¹⁸ Diego Zuluaga, “Should Cryptocurrencies be Regulated like Securities”, *CATO Institute*, 25 June 2018, available at <<https://www.cato.org/cmfa-briefing-paper/should-cryptocurrencies-be-regulated-securities#how-cryptocurrencies-work>> last accessed 27 July 2021.

traditional definition of security that has worked for a long time”, simply for the sake of accommodating cryptocurrency.¹⁹

2.3. What benefits do cryptocurrencies offer?

As explained above, regulatory paralysis has, in part, been caused by difficulties classifying cryptocurrency. However, it has been exacerbated by divided views on whether cryptocurrencies offer any benefits and if they do, what these might be. This is important because if cryptocurrencies do not have inherent value or deliver real benefits, they are unlikely to stand the test of time, making it difficult for governments to justify developing a comprehensive regulatory regime (a resource-intensive exercise).

According to Zanten, a financial markets historian at Kings College London, “*cryptocurrencies are still solutions looking for a problem*”, meaning they do not offer any practical advantages. He explained that crypto-sympathisers should do more than appeal for time or say that the trajectory of cryptoassets resembles the early days of the internet.²⁰ By his summation, cryptocurrencies can be traced back to the work of American cryptographer David Chaum, whose dissertation “*Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups*” was published in 1982.²¹ This work proposed almost every element of the blockchain (later outlined in the White Paper).²² Chaum also founded Digicash in 1989, an electronic money company which created the first digital currency. In this way, digital currencies clearly do predate bitcoin and claims that this asset needs time to mature are questionable.

On the other hand, crypto-fans see the proliferation of online currencies as the modern day equivalent of the 19th century gold rush. Others take a more moderate approach, arguing that cryptocurrencies *could* pave the way for cheaper, faster payments, making it easier for people to store money and make purchases. For example, while the Reserve Bank of India has voiced concerns over the financial

¹⁹ Kate Rooney, “SEC chief says agency won’t change securities laws to cater to cryptocurrencies”, *CNBC*, 6 June 2018, available at: <<https://www.cnbc.com/2018/06/06/sec-chairman-clayton-says-agency-wont-change-definition-of-a-security.html>> last accessed 27 July 2021.

²⁰ Joseph von Zanten, “Letter: cryptocurrencies are still solutions looking for a problem”, *Financial Times*, 6 July 2021, available here: <<https://www.ft.com/content/6f63d6f0-f040-4795-a45d-d65103f48348>> last accessed 26 July 2021.

²¹ David Lee Chaum, “Computer Systems Established, Maintained and Trusted by Mutually Suspicious Groups”, *University of California, Berkeley*, 4 April 1982, available at: <<https://nakamotoinstitute.org/static/docs/computer-systems-by-mutually-suspicious-groups.pdf>> last accessed 26 July 2021.

²² Alan Sherman, Farid Javani, Haibin Zhang, and Enis Golaszewski, “On the Origins and Variations of Blockchain Technologies”, 14 October 2018, available at: <<https://arxiv.org/pdf/1810.06130.pdf>> last accessed 26 July 2021.

stability risks of cryptocurrencies, it is also investing in blockchain technology and seeking to launch its own digital currency.

While the inherent value of cryptocurrency may be debateable, the speed with which it has infiltrated financial markets and its broadening appeal are not. This trend has accelerated during the pandemic, given that more of daily life has been conducted online, and given consumers have had more time to contemplate investments during lockdowns. As such, there has been a cryptocurrency boom.

3. The pros and cons of regulation

3.1. *Criminal activity*

A compelling reason to regulate cryptocurrencies is the way in which they facilitate criminal activity. It is widely reported that drug-dealers use bitcoin to move money around and take payments.²³ A study by cyber-security firm Chainalysis found that darknet markets (online platforms that offer illegal goods such as drugs) set a cryptocurrency revenue record in 2020 - they received \$1.7 billion worth of cryptocurrency (up from \$1.3 billion in 2019).²⁴ Reuters has also reported that bitcoin is frequently used by drug gangs such as the Jalisco New Generation Cartel and the Sinaloa Cartel (two semi-militarised criminal groups in Mexico).²⁵ Putting cash into the mainstream banking system (designed to detect laundered proceeds) is perilous, as is transporting hard cash across borders. Cryptocurrency offers another way to get profits back to the cartels and makes drug-related crime easier to perpetrate.

According to Santiago Nieto, drug gangs use a technique called “smurfing” - that is, splitting criminal proceeds into small amounts and depositing these smaller chunks into various bank accounts, so that compliance alarm bells aren’t triggered. Those accounts are then used to purchase bitcoin online, concealing the origin of the funds and allowing criminals to trade bitcoin between themselves. In this way, bitcoin

²³ “New technology has enabled cyber-crime on an industrial scale”, *The Economist*, 8 May 2021, available at: <<https://www.economist.com/international/2021/05/06/new-technology-has-enabled-cyber-crime-on-an-industrial-scale>> last accessed 27 July 2021.

²⁴ “The 2021 Crypto Crime Report” *Chainalysis*, 16 February 2021, available at: <<https://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis-Crypto-Crime-2021.pdf>> last accessed 27 July 2021.

²⁵ Diego Oré, “Insight - Latin American crime cartels turn to crypto to clean up their cash”, *Reuters*, 8 December 2020, available at: <<https://www.reuters.com/article/mexico-bitcoin-insight-idUSKBN2811KD>> last accessed 30 July 2021.

offers cartels a new way to launder dirty money and pay associates, as well as allowing traffickers to avoid the risks of transporting hard cash.²⁶

Other kinds of cryptocurrency-enabled crime have grown dramatically during the pandemic. The growth in ransomware attacks (where a target's files are locked up until funds are paid) is particularly pronounced. Although this phenomenon is not new, such attacks used to be crude and small scale with hackers focused on ordinary people's computers and demanded modest sums. Recently, victims include companies, governments and law enforcement agencies. Mimecast (a cybersecurity provider) reported that during 2020 more than 6 in 10 of the companies that it surveyed suffered a ransomware attack - a marked increase from 2019, when only 50% of respondents reported the same. Moreover, as a result of these 2020 attacks, organisations experienced (on average) 6 days of downtime - more than double compared to 2019.²⁷ Importantly, modern day ransom demands are mostly made in cryptocurrency. In its 2021 report, Chainalysis said that the amount paid in cryptocurrency ransoms over the course of 2020 was \$350 million (a 311% increase, as compared to 2019).²⁸

To give an example of how damaging these ransom attacks can be, at the end of 2019, the British currency trader Travelex was targeted by hackers. This led to the company sending 285 bitcoin (then worth around \$2.3 million) to the hackers. This episode contributed to a loss of £25 million the following quarter. The company went into administration a few months later, leading to the loss of 1,300 jobs. While various factors were at play, the ransomware attack is understood to have played a significant role in the company's collapse. The company's administrators noted that the cyber-attack "acutely impacted the business".²⁹

Due to the abundance of evidence that crypto-exchanges are being used to move dirty money, regulatory attempts have been made. In 2019, the Financial Action Task Force ("FATF") proposed - and finalised - guidance urging nations to implement Know Your Client ("KYC") requirements for all crypto-exchanges. This guidance defined 'virtual asset service providers' as businesses that transfer funds in the form of cryptocurrency (i.e. crypto-exchanges). It specified that these businesses should have KYC information for all transaction parties. Although the roll-out of these rules

²⁶ Diego Oré, "Insight - Latin American crime cartels turn to crypto to clean up their cash", *Reuters*, 8 December 2020, available at: <<https://www.reuters.com/article/mexico-bitcoin-insight-idUSKBN2811KD>> last accessed 30 July 2021.

²⁷ "Mimecast - The State of Email Security Report (2021)", *Mimecast*, available at: <<https://www.mimecast.com/globalassets/documents/ebook/state-of-email-security-report-2021.pdf>> last accessed 27 July 2021.

²⁸ "The 2021 Crypto Crime Report" *Chainalysis*, 16 February 2021, available at: <<https://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis-Crypto-Crime-2021.pdf>> last accessed 27 July 2021.

²⁹ Kalyeena Makortoff, "Travelex falls into administration, with loss of 1,300 jobs", *The Guardian*, 6 August 2020, available at: <<https://www.theguardian.com/business/2020/aug/06/travelex-falls-in-to-administration-shedding-1300-jobs>> last accessed 30 July 2021.

is in its infancy, many countries are beginning to scrutinise crypto-exchanges more closely. For example, China has imposed an outright ban on crypto-exchanges and South Korea has brought new anti-money laundering rules into effect, resulting in the decision of a prominent crypto-exchange (OKEx) to close operations there.

Financial institutions across the globe spend billions on anti-money laundering efforts and there is increasing pressure on crypto-exchanges to follow suit. As evidenced by OKEx's move, some companies are responding to greater regulatory scrutiny by 'jurisdiction hopping'. Such is short-sighted and damages the credibility of the crypto-industry. Regulatory controls drive up costs and require the hiring of compliance personnel. However, they will also broaden the sector's appeal, bolster investor confidence and encourage growth. In the words of the Ontario Securities Commission's Chief Executive Officer, Grant Vingo, "*firms that have nothing to hide should embrace this opportunity to enhance confidence in their business by seeking registration and appropriate oversight*".

3.2. Price volatility and the cryptocurrency "bubble"

Greater regulation has another major advantage for investors and consumers - it will decrease uncertainty and likely temper price volatility. To be sure, the price of cryptocurrencies (like all commodities) is impacted by the zeitgeist and unquantifiable consumer appetites. To quote Sir Isaac Newton, "*I can calculate the motion of heavenly bodies but not the madness of people*". However, in the case of cryptocurrency, large price fluctuations have been caused (at least in part) by regulatory uncertainty. Indeed, if we have learned nothing else from the devastation wrought by COVID-19, it is that uncertainty is bad for business and for markets.

This point is important because price volatility has prevented bitcoin from becoming a reliable store of value and undermined mainstream investor participation. To grasp how volatile pricing has been, you need look no further than bitcoin's trajectory over the last three years. In December 2017, the price of bitcoin stood at almost \$20,000, only to plummet to below \$10,000 the following month (a dramatic decline of almost 50%). This downwards trend continued throughout 2018, leading many to speculate that the bitcoin bubble had burst. Indeed, The Economist newspaper wrote an article entitled "*The rise and fall of bitcoin*".

According to some, the degree of volatility we have seen indicates that cryptocurrencies and their pricing are inherently irrational. In 2017, the former chairman of the U.S. Federal Reserve, Alan Greenspan, likened bitcoin to an "irrational" war-time currency, which came into use in 1775 and was worthless by 1782. This paper-based legal tender was used during the American Revolutionary War and was not backed by a commodity such as gold - in this way, it had no inherent worth and could not stand the test of time. In Mr Greenspan's summation, it is likely

that bitcoin (which ultimately has no value) will also be consigned to the dustbin of financial history. He went to say that bitcoin is a “*fascinating example of how human beings create value*”, which is not always rational or sustainable.³⁰

Putting aside the question of whether cryptocurrencies have inherent worth, the fact remains that they have penetrated mainstream market activity and significant gains (and indeed losses) are being made. With this in mind, it is the duty of regulators to step in and provide confidence, stability and better consumer protection. The need for regulatory input is best captured by the way in which many financial experts are talking about cryptocurrencies. While many commentators have characterised the bitcoin market as a bubble, others have issued more serious warnings. For example, in 2017 JP Morgan Chase’s CEO called bitcoin a “fraud” that will “blow up”. He went on to say that he would fire any trader known to be trading the currency for being “stupid”.³¹

3.3. The downsides to regulation - market activity, innovation and jurisdiction hopping

Arguably, however, greater regulation will chill market activity and spook investors. By way of example, the new head of the SEC, Gary Gensler, recently said that “*bitcoin and other cryptocurrencies brought new thinking to payments but raised new issues of investor protection that [the SEC] still need to attend to*”. During his speech to the Senate Banking Committee, Gensler also promised to provide “*guidance and clarity*” in this area. Almost immediately, the price of bitcoin fell by 3%. In some ways, this is hardly surprising - indeed, it is conventional wisdom that when regulators intervene, markets react and usually negatively.

This assumption is further supported by events in China. When reports began to circulate that Chinese regulators would ban the country’s crypto-exchanges, bitcoin’s price fell by 10% in a single day. A comparable price decline followed in May 2021, when China officially banned companies from providing crypto-related services. While China had signalled for years that it wanted to ban bitcoin, May’s announcement was dramatic and authorities clearly intend to enforce the ban - indeed, there was a flurry of arrests in Summer 2021 relating to people using cryptocurrencies in allegedly nefarious ways.³²

³⁰ Sujha Sundararajan, “Greenspan Likens ‘Irrational’ Bitcoin to Revolutionary War Currency”, *CoinDesk*, 7 December 2017, available at: <<https://www.coindesk.com/greenspan-likens-irrational-bitcoin-to-revolutionary-war-currency>> last accessed 30 July 2021.

³¹ Stan Higgins, “Jamie Dimon: Bitcoin Is a Fraud”, *Coin Desk*, 12 September 2017, available at: <<https://www.coindesk.com/jamie-dimon-bitcoin-fraud>> last accessed 30 July 2021.

³² MacKenzie Sigalos, “China’s war on bitcoin just hit a new level with its latest crypto crackdown”, *CNBC*, 7 July 2021, available at: <<https://www.cnbc.com/2021/07/06/china-cracks-down-on-crypto-related-services-in-ongoing-war-on-bitcoin.html>> last accessed 28 July 2021.

However, a recent article by academics at the Wharton School has challenged this assumption.³³ Their research shows that regulatory announcements in relation to cryptocurrencies have not, in practice, affected crypto-trading volume. Nor have such announcements had a significant and lasting impact on price. In fact, this article goes as far as to say that in all but the most extreme cases (like China's all-out ban) concerns over regulatory action are "illusionary". Far from chilling activity and stifling innovation, regulation can have the opposite effect because "*clear rules promote market trust*".³⁴

Others argue that regulatory efforts will stifle the technology associated with cryptocurrency, before it is able to deliver the anticipated benefits. Crypto-enthusiasts see this is an unfair way to treat a new and innovative technology. However, if you place cryptocurrencies in the context of *other* new technologies that have emerged in the 21st century this perspective is short-sighted. Gene editing, high finance derivatives and internet platforms such as Facebook have all been the subject of regulatory action.

New technologies do not grow and evolve in isolation, without government oversight - that would be irresponsible. To grasp this point, look no further than America's love affair with the automobile. When regulatory efforts began in the sixties (in response to catastrophic fatality rates) they were extremely divisive. Today, the idea of driving under the influence or without a seat belt is laughable. At the time, however, there were those who sought to block regulation in the name of innovation, freedom and cost-cutting. The way in which safety regulations have developed in the auto-industry underline that, while ground-breaking technologies can be wondrous, they must be supported by regulation. For the safety of consumers and investors, innovation and regulation must be in continuous dialogue. Cryptocurrencies simply appear to be next in line for that conversation.

Cryptocurrency advocates also assert that regulatory attempts will be futile, because trading activity will simply shift to other (more lenient) jurisdictions. As evidenced by Binance's *modus operandi*, there may be some truth in this. Since its inception in 2017, Binance (the world's largest cryptocurrency exchange in terms of daily trading volume) has moved operations several times - from China to Japan and then onto Malta. Aptly summed up in a recent Financial Times article, "*Changpeng Zhao's company Binance is everywhere and yet based nowhere*". Rather than jumping through regulatory hoops (which requires time, resources and compliance lawyers), Binance has simply shifted its operations to more permissive jurisdictions. However, this strategy is short sighted. While the Chinese ban on crypto-exchanges is the most extreme example, in 2021 we have seen regulators across the globe

³³ Brian Feinstein and Kevin Werbach, "Don't fear Cryptocurrencies, Manage Them", *The New York Times*, 14 April 2021, available at: <<https://www.nytimes.com/2021/04/14/opinion/coinbase-ipo-cryptocurrencies.html>> last accessed 30 July 2021.

³⁴ *Ibid.*

clamp down on cryptocurrencies - soon there may be nowhere left for Binance to go.

4. 2021 - the year that regulators pushed back

In June 2021, the UK's Financial Conduct Authority (the "FCA") issued a warning to Binance. The FCA ruled that Binance cannot conduct any "regulated activity" in the UK because it is not registered with it.³⁵ At first blush, this announcement appears to be of little consequence - Binance is domiciled in the Cayman Islands and has entities dotted around the world to facilitate its operations. Notwithstanding this announcement, UK customers may simply use the Cayman Islands-based exchange to trade in cryptocurrencies.

This move by the FCA is also part of a wider 2021 trend - regulators around the world have begun to push back against cryptocurrency platforms. Binance has attracted intense scrutiny from a host of government agencies. The following four examples contextualise this. First, in April 2021, the SEC issued a warning to American consumers about Binance and its operations. Second, in June 2021, the Ontario Securities Commission alleged that Binance (as well as various other crypto-platforms) has failed to comply with province regulations. The company promptly ceased operations in Canada, announcing on 25 June 2021 that "*Binance can no longer continue to service Ontario-based users. Ontario-based users are advised to take immediate measures to close out all active positions by December 31, 2021*".³⁶ Third, on 25 June 2021, Japan's Financial Services Agency warned Binance (for the second time in three years) that it was operating in Japan without the necessary permissions. Finally, on 2 July 2021, Thailand's financial watchdog filed a criminal complaint against Binance, for operating a digital asset business without a licence. According to Thailand's Securities and Exchange Commission, it warned Binance about its activities in April. After receiving no response, the watchdog then decided to file a criminal complaint.³⁷

According to Tom Keatinge of The Royal United Services Institute (a British defence and security think tank), "*crypto-exchanges are the frontier between the dark web and the regulated fiat world*". With this in mind, it is hardly surprising that Binance

³⁵ "Consumer warning on Binance Markets Limited and the Binance Group", *Financial Conduct Authority*, 26 June 2021, available at: <<https://www.fca.org.uk/news/news-stories/consumer-warning-binance-markets-limited-and-binance-group>> last accessed 28 July 2021.

³⁶ "Terms of Use Review", *Binance*, 25 June 2021, available at: <<https://www.binance.com/en/support/announcement/ba03469c86f34546bd25faf414730733>> last accessed 29 July 2021.

³⁷ "Crypto exchange Binance hit by criminal complaint from Thai regulators", *Reuters*, 2 July 2021, available at: <<https://www.reuters.com/technology/thailand-sec-files-criminal-complaint-against-crypto-exchange-binance-2021-07-02/>> last accessed 29 July 2021.

has been the focus of the recent regulatory offensive. Reflecting on the FCA's announcement, Mr Keatinge went on to say that the British watchdog should be "*congratulated for cracking down on Binance and putting the fear of God in others*".

A post-COVID-19 future has significant, financial difficulties for all Governments around the world. Does this author consider that this might focus legislative minds on a thus far unregulated US\$1 Trillion Industry? Just ask Google.

About the Author



Kate McMahon 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."

Contact Kate McMahon: T. 02075838392; E. katemcmahon@emmlegal.com

Coming to Terms with Crypto

Christopher Weil, Sean Anderson and
Craig Heschuk

Abstract

In this article, Christopher Weil, Managing Partner of Mintz Group, Sean Anderson, Director of Mintz Group, and Craig Heschuk, Executive Vice President of GreyList Trace consider the complex world of cryptocurrency, its regulation and developments across jurisdictions, and its impact on digital asset recovery cases. They highlight and explain some of the technical nuances, and consider how various tools have developed relevant to investigations.

Introduction

What the ultimate role of cryptocurrency should be is one of the most important issues facing the global financial community today. The uncertainty and flux around this question generates considerable noise and makes it challenging for attorneys who advise clients on asset recovery to develop a consistent approach to cryptocurrency. However, once that noise is filtered out, a clearer picture of how to respond to crypto quickly emerges.

Crypto is Here to Stay

Much of the distraction around crypto stems from the lingering debate over whether it should be considered a legitimate asset class, given crypto's considerable market gyrations, the risk of investing in a fraudulent project and regulatory uncertainties. But while this debate has raged since crypto's inception, it is being increasingly resolved in crypto's favor. If crypto's market value has fluctuated considerably, the integration of crypto into the mechanics of the financial system has maintained a relatively steady upward momentum for the past several years. Just in recent weeks, for example, a Bitcoin futures ETF has made its debut on U.S. exchanges and U.S. banks have begun offering a cryptocurrency custody service for large investment

managers. Among emerging markets, several countries are considering following El Salvador's lead and adopting Bitcoin as legal tender in the near future.

Similarly, while government officials may sound the alarm over crypto's risks and regulatory issues, most of those pronouncements in the U.S. and elsewhere implicitly acknowledge crypto's continued existence. Even China's official opposition to crypto needs to be seen in the context of the competition it poses to the recently introduced digital yuan. Even in the best of cases, the process of regulation catching up to innovation is messy. It is all the more so when that process involves trying to regulate something that was designed from the start to be unregulated. How that fundamental, structural conflict will be resolved is far from clear. Nonetheless, it is increasingly safe to say that crypto's role in the global financial system is a question of *how* and *when*, not *if*.

Piercing Crypto's Aura of Impenetrability

Once we accept that crypto is here to stay, we must then confront crypto's aura of impenetrability. But here, too, a much more manageable reality emerges once the noise is ignored. All currency is based on trust, and crypto is no exception. Instead of the backing of a government, crypto's trust is based on the transparency of its blockchain, a public ledger of transactions stored in a continuous chain of time-stamped blocks, distributed across thousands of computers, providing a record that is essentially permanent, immutable and highly resistant to tampering.

Crypto's much-discussed privacy stems from the fact that while the transactions are listed on the blockchain for all to see, the parties to each transaction are identified only by a long randomly generated 24-plus-character pseudonym, which is not directly tied to a user's identity. However, such privacy is compromised whenever the user attempts to convert cash to crypto on an exchange, which is still necessary for most users when they want to invest in a cryptocurrency or conduct a transaction. Conversely, the same vulnerability exists when converting crypto to cash, when users want to move profits to the traditional bank account.

These "on-ramps" and "off-ramps" to the crypto blockchain are both the weakest links in the chain and the leverage points for any investigation of cryptocurrency assets.

Entering and exiting the cryptocurrency ecosystem generally requires using a crypto exchange, such as Coinbase, Kraken or Binance, which act as on-ramps and off-ramps to the pseudonymous blockchain. These exchanges, which began as part of crypto's opaque libertarian origins, have evolved to become firmly planted in the world of mainstream institutions—allowing lawyers, investigators, regulators and law enforcement to bring to bear the traditional tools of subpoenas and court orders, and get the information necessary to link fiat and crypto exchange accounts and

follow the money. Indeed, in the case of *U.S. vs. Gratkowski* [2020] the Fifth Circuit ruled that law enforcement does not even need a warrant to demand customer records from a crypto exchange, using the same Fourth Amendment exclusion that the courts previously applied to bank records.

It is important to note, however, that while crypto exchanges are not immune from legal action, they are not yet subject to the same regulatory scrutiny as banks and brokerages. Some offshore exchanges are less than cooperative in complying with law enforcement and civil court requests; others are lax in applying KYC and other crime-prevention measures. In general, however, cryptocurrency exchanges have been tightening their KYC rules and lowering the amount of crypto that can be sent without providing some identifying information.

In addition to the information that can be gleaned from crypto exchanges, a new generation of digital investigative tools is dramatically increasing the capacity to trace and recover crypto by scraping the massive amounts of data on blockchains to identify suspicious transaction patterns or addresses and allow investigators to track stolen or fraudulent crypto to exchanges, where the recipient could then be identified through civil court requests. Given the nature of the blockchain, these transactions can even be monitored and traced years later, when stolen crypto that had been dormant starts to move again. The seizure of crypto linked to theft or fraud is now sufficiently commonplace that the U.S. Justice Department recently awarded a contract for the handling of the digital assets seized by the U.S. Marshals Service.

The Crypto Arms Race

These advances in “domesticating” crypto pave the way for it to be integrated into the global financial system. At the same time, however, other technological innovations help keep crypto rooted to its undomesticated, off-the-grid origins. For example, the emerging sector of “decentralized finance” or “DeFi” protocols leverage “smart contracts” to bypass crypto exchanges entirely, allowing for more opaquely pseudonymous transactions. Despite their legitimate uses, bad actors are also using DeFi to avoid centralized exchanges and increase the difficulty of tracing stolen crypto. They are even engaging in strategies akin to money laundering, in which “dirty” crypto acquired through fraud or theft is used as collateral on a DeFi platform to obtain a loan made in “clean” crypto that can be moved back through centralized exchanges.

The playing field for digital asset recovery is thus highly dynamic, similar to the arms race between hackers and cybersecurity experts. And just as crypto has its libertarian legacy, the Internet’s evolution from obscure niches in government and academia to global ubiquity was intertwined with a hacking culture with heavy

anarchist undertones. That hacking culture did not prevent the internet’s trajectory, but it did require an ever-evolving corpus of regulations, resources and best practices to guide actions and mitigate risk.

Crypto is in the early stages of a similarly bumpy evolution. As with cybersecurity, the prudent course for those helping clients recover assets in the crypto realm is not to wait for all of crypto’s uncertainties to be resolved—because they may never be—but rather to adapt existing tools where possible and innovate where needed, as this new domain becomes just one more element in the global asset recovery toolkit. The tried and true methods of asset tracing and recovery, mixing both open source and traditional investigative steps with judicially-sanctioned discovery, apply to the crypto realm. Chief amongst these tools is the opportunity afforded by leveraging disclosures at the on-ramps and off-ramps of the blockchain.

About the Authors



Sean Anderson is a director at the Mintz Group, heads the Mexico City office and works closely with the Mintz Group’s Washington D.C. office. He works in our Latin American practice and has experience conducting complex litigation, integrity due diligence and asset tracing investigations.

Sean has conducted numerous investigations throughout Latin America, with a particular emphasis on the infrastructure, energy and financial services sectors. Recently, he undertook comprehensive pre-deal investigations into companies in Honduras, Guatemala and Mexico, which uncovered ties to organized crime, large-scale tax fraud and money-laundering.

Sean has also led internal investigations into contract fraud and bribery at a large mining company and undisclosed conflicts of interest leading to multimillion-dollar distressed loans at a multinational financial institution. He also manages cryptocurrency-related investigations on behalf of clients involved in multimillion-dollar lawsuits. Sean is fluent in English, Spanish and proficient in French.

Contact Sean Anderson: SAnderson@mintzgroup.com



Chris Weil is managing partner of the Mintz Group's Washington, D.C. office specializing in complex litigation and public-policy disputes. He co-heads the firm's international asset tracing unit and leads the firm's antitrust practice. His practice focuses exclusively on complex disputes – ranging from corporate litigation to international arbitration claims to trade disputes and corporate reputation management.

Chris has conducted investigations in a wide variety of industries, from manufacturing to logistics to the financial services sector, and has worked as the lead investigator in some of the largest global asset investigations in recent years. He was recognized as a leading practitioner in *Who's Who Legal Asset Recovery Experts* for five consecutive years beginning in 2016 and he was commended for his "highly intelligent and responsive manner."

Chris also serves on the Editorial Advisory Board of the *Journal of Enforcement of Arbitration Awards* published by JurisNet.

Contact Chris Weil: cweil@mintzgroup.com

Craig Heschuk is Executive Vice President at Greylist Trace. Craig 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.



Contact Craig Heschuk: T +1 778 363 8954; E. craig.heschuk@greylisttrace.com

Cryptocurrency Disputes - Jurisdictional Challenges and Novel Solutions

Danny Ong and Stanley Tan

Abstract

Cases of cryptocurrency fraud raise knotty issues of jurisdiction not only because of the decentralised nature of cryptocurrency, but also because the parties involved are often spread across multiple jurisdictions. As a result, before victims of cryptocurrency fraud can obtain any relief against the unknown fraudsters or the cryptocurrency exchanges embroiled in the fraud, they would first have to convince a court that it has the necessary jurisdiction over the defendants. In this article, Danny Ong and Stanley Tan of Rajah & Tann Singapore LLP considers some of the jurisdictional challenges commonly faced by victims of cryptocurrency fraud before proffering possible solutions to overcoming them.

Introduction

The surge in cryptocurrency's popularity has unfortunately seen a corresponding increase in related fraud cases. While courts around the world are generally sympathetic and willing to assist victims of cryptocurrency fraud, they would first have to be convinced that they have the jurisdiction to do so. Establishing such jurisdiction may at first glance seem challenging because cryptocurrency fraud cases involve a decentralised digital asset, unknown fraudsters, and cryptocurrency exchanges that could be operating out of multiple jurisdictions. This article considers some of the challenges that victims suing in Singapore are likely to face when attempting to establish jurisdiction over (i) unknown fraudsters and (ii) cryptocurrency exchanges embroiled in the fraud, and considers some solutions in response to these challenges.

Establishing Jurisdiction Over Unknown Fraudsters

The need to establish jurisdiction over unknown fraudsters often arises after victims have traced the misappropriated cryptoassets into accounts held with

cryptocurrency exchanges. As cryptocurrency exchanges are generally reluctant to freeze accounts for prolonged periods without a court order, victims will usually need an urgent court order to ensure that the cryptoassets in those accounts remain frozen until their claim has been adjudicated. However, as the identities of these account holders are typically unknown, victims will have to convince the court that it has jurisdiction to make freezing orders against unknown defendants.

At first blush, this might seem implausible because defendants should ordinarily be named in any claim against them. In Singapore, for example, the need to identify defendants seems to be implied in section 16(1) of the *Supreme Court of Judicature Act*¹ that requires defendants to be served with the originating process before jurisdiction can be established against them. The prescribed forms for commencing an action in Singapore also seem to require that the defendants' names and addresses be stated².

However, there is a strong case to be made for Singapore Courts having jurisdiction against unknown defendants (and indeed, we have successfully persuaded the Singapore Court to grant freezing orders as against these unknown defendants' assets):

- (i) there is no express prohibition to claiming against unknown defendants. In fact, O1r7 of the Rules of Court³ ("ROC") expressly states that the prescribed forms can be used "*with such variations as the circumstances ... require*". The Singapore Court also has the power under O2r1(1) ROC to cure any procedural defects, which should include those relating to the identity of the defendants;

- (ii) although unknown defendants cannot be personally served with the originating process, they can be served via substituted means. Under O62r5 ROC, substituted service is allowed if personal service is impracticable and the mode of substituted service is effective in notifying the defendants of the claim. As it is clearly impracticable to personally serve unknown defendants, all that victims require is an effective mode of substituted service. One possible mode involves emailing the owners of the accounts containing the misappropriated cryptoassets, whose emails can be obtained via disclosure applications against the relevant cryptocurrency exchanges⁴;

¹ (Cap 322, 2007 Rev Ed Sing).

² See forms 2, 4 and 5 of Appendix A of the Rules of Court (Cap 322, 2014 Rev Ed Sing).

³ (Cap 322, 2014 Rev Ed Sing).

⁴ *AA v Persons Unknown* [2020] 4 WLR 35 ("AA") at [75]; *Ion Science Limited v Duncan Johns* [2020] EWHC 3688 (Comm) ("*Ion Science*") at [23].

- (iii) the courts of countries like the United Kingdom (“UK”), Canada⁵, Hong Kong⁶, and recently Malaysia⁷, have all claimed jurisdictions over unknown defendants. For example, the UK Supreme Court has affirmed that claims can be made against an unknown defendant provided he is “*described in a way that makes it possible in principle to locate or communicate with him and to know without further inquiry whether he is the same as the person described in the claim form*”⁸. In fact, this jurisdiction has recently been invoked in two UK decisions involving cryptocurrency fraud⁹, where the UK Court granted urgent reliefs against “persons unknown” preventing them from dealing with the misappropriated cryptoassets held in their accounts with various cryptocurrency exchanges; and
- (iv) the Singapore Court will have no hesitation in developing the law to adapt to technological developments, so as to prevent fraudsters from evading justice on procedural grounds just because they are able to conceal their identities.

Besides convincing the court that it has jurisdiction to grant orders against unknown defendants, victims must also convince the court that it has jurisdiction to determine the claims against them. However, this might seem challenging because jurisdiction is traditionally determined by “territorial connecting factors” like where the wrongful acts were committed or where the damage was suffered¹⁰, and claims involving intangible property like cryptocurrency have “placed a strain upon this territorial paradigm”¹¹. For example, the victim’s domicile might not be where the wrongful acts were committed as the fraudsters could have been operating from a different jurisdiction. The victim’s domicile might also be different from the location at which the cryptoassets were held, for they might have been held in the

⁵ *Jackson v Bubela* [1972] 5 WWR 80; *Golden Eagle v International Organization of Masters* [1974] B.C.J. No. 614; *Busseri v John Doe* [2014] O.J. No. 605; *Voltage Pictures LLC v John Doe* [2015] 2 F.C.R. 540.

⁶ *University of Hong Kong v Hong Kong Commercial Broadcasting Co Ltd* [2016] 1 HKLRD 536; *MTR Corporation Ltd v Unknown Persons* [2019] 5 HKC 260.

⁷ *Zschimmer & Schwarz GMBH & Co Kg Chemische Fabriken v Persons Unknown & anor* [2021] MLJU 178

⁸ *Cameron v Liverpool Victoria Insurance Co Ltd* [2019] 3 All ER 1 at [13].

⁹ *Ion Science*, *supra* note 4; *AA*, *supra* note 4

¹⁰ see for example, Order 11 rule 1(f) of the Rules of Court (Cap 322, 2014 Rev Ed Sing), Article 7(2) of the Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast), Paragraph 9 of Practice Direction 6B which supplements Part 6 of the *Civil Procedural Rules* (UK), and Rule 10.42 of the *Federal Court Rules 2011* made under the *Federal Court of Australia Act 1976* (Cth).

¹¹ Andrew Dickinson, “Cryptocurrencies And The Conflict Of Laws” in David Fox & Sarah Green (eds), *Cryptocurrencies in Public and Private Law* (Oxford University Press, 2019) at [5.08].

servers of a cryptocurrency exchange located in a different jurisdiction before they were misappropriated.

Despite these difficulties, there are good bases for establishing jurisdiction against unknown fraudsters. For example, victims domiciled Singapore may rely on the following arguments to establish jurisdiction under O11r1(f)(ii) ROC, on the basis that the damage was suffered in Singapore:

- (i) under O11r1(f)(ii) ROC, there is a presumption that the damage is suffered in the jurisdiction where the victim is incorporated¹². Although this presumption applies to companies, there is no reason why it cannot be extended to the domiciles of victims who are natural persons;

- (ii) regardless of where the servers containing the victim’s cryptoassets might be located, the Singapore Court may be inclined to adopt the view that cryptoassets are located in the domicile of the person or company who owns it. Therefore, any damage caused by cryptocurrency fraud would be suffered in the victim’s domicile as that would be where the cryptoassets were misappropriated from. This analysis by Professor Andrew Dickinson¹³ has been recognised by the UK Court as potentially being the “correct analysis”¹⁴ and could thus be sufficient for establishing jurisdiction in Singapore as well;

- (iii) in assessing where damage was suffered in cases of cryptocurrency fraud, reference should only be taken from the victim’s domicile because any other analysis would be too arbitrary. For example, it would be unpalatable if reference is taken from the location of the servers containing the victim’s cryptoassets because that location is not publicly known and could practically be anywhere in the world, possibly even in multiple jurisdictions. As the rules on jurisdiction should pursue the objective of foreseeability¹⁵, taking reference from the victim’s domicile in cryptocurrency fraud cases would be preferable because it would prevent a “lottery of jurisdiction”¹⁶ where proceedings have to be commenced wherever the servers happen to be; or

¹² *Man Diesel & Turbo SE and another v IM Skaugen SE and another* [2020] 1 SLR 327 (“*Man Diesel*”) at [78].

¹³ *Andrew Dickinson, supra* note 11 at [5.108]

¹⁴ *Ion Science, supra* note 4 at [13].

¹⁵ *Wintersteiger AG v Products 4U Sondermaschinenbau GmbH* [2012] ECLI:EU:C:2012:220 at [36]; Lord Collins & Jonathan Harris, eds, *Dicey, Morris & Collins on the Conflict of Laws*, 15th ed (London, UK: Sweet & Maxwell, 2018) at Chapter 11.

¹⁶ *Skyrotors Ltd v Carriere Technical Industries Ltd* [1979] O.J. No. 3129 at [14].

- (iv) if the victim had funded the purchase of his misappropriated cryptoassets with a bank account situated in the jurisdiction of their domicile, that can constitute a ground for arguing that the damage was suffered there as well¹⁷.

Establishing Jurisdiction Over Cryptocurrency Exchanges

Victims of cryptocurrency fraud will often also need to seek disclosure orders against cryptocurrency exchanges that received the misappropriated assets. This is for the purpose of identifying the unknown defendants and tracing the cryptoassets. As cryptocurrency exchanges often operate out of a group of companies spread across multiple jurisdictions, disclosure applications are usually commenced against the parent company of the group. For example, disclosure applications against Binance would generally be made against Binance Holdings Ltd, and those against Kraken would be made against Payward Ventures Inc¹⁸. However, establishing jurisdiction over these companies may pose difficulties as no claim of wrongdoing is being made against them, and they may be based outside the jurisdiction in which the application is sought.

Nevertheless, there may still be territorial connecting factors that can be utilised to establish jurisdiction against them. For example, in Singapore, jurisdiction could be established under O11r1(a) ROC on the basis that the parent company is “carrying on business” in Singapore. As many cryptocurrency exchanges offer their services and have offices and employees in Singapore, obtaining sufficient evidence to establish a good arguable case¹⁹ of jurisdiction should not prove too difficult.

Alternatively, if the parent company is based in a jurisdiction that allows for disclosure orders to be granted in aid of foreign proceedings, commencing a separate disclosure application there could also be an option. For example, this option could be available for disclosure applications against exchanges incorporated in the Cayman Islands, as the Cayman Court has recently held that a *Norwich Pharmacal Order* can be granted in support of foreign proceedings²⁰.

¹⁷ *Ion Science*, *supra* note 4 at [13]; *AA*, *supra* note 4 at [68].

¹⁸ *Ion Science*, *supra* note 4 at [3].

¹⁹ *Man Diesel*, *supra* note 12 at [30].

²⁰ William Jones & Nour Khaleq, “The Cayman Islands Court of Appeal finds that Norwich Pharmacal relief is available in aid of foreign proceedings” (Ogier, 12 May 2021), <<https://www.ogier.com/publications/the-cayman-islands-court-of-appeal-finds-that-norwich-pharmacal-relief-is-available-in-aid-of-foreign#>> accessed 22 July 2021.

Conclusion

In conclusion, the jurisdictional challenges that arise in cryptocurrency fraud cases are certainly not insurmountable, and strong arguments may be made within the existing legal frameworks to help victims establish jurisdiction. While it is hoped that a global regulatory framework governing the cryptocurrency industry will assist in resolving some of these challenges, victims ought to be encouraged by the fact that innovative solutions may be found within the current legal framework.

About the Authors



Danny Ong leads Rajah & Tann's Fraud, Asset Recovery & Investigations practice. He has advised and represented various state-owned companies, governmental agencies, international financial institutions, and liquidators, in the investigation and prosecution of claims involving complex multi-jurisdictional corporate and commercial fraud and breaches of fiduciary duties, enforcement of foreign judgments, and the recovery and tracing of assets globally, involving billions of dollars.

In the last decade, he has been involved in some of the highest-profile cross-border fraud matters to be seen in Singapore and the region, including more recently, matters involving the recovery of cryptocurrencies.

Contact Danny Ong: danny.ong@rajahtann.com

Stanley Tan is an associate at Rajah & Tann Singapore LLP's Dispute Resolution team, where he specialises in international commercial disputes and investigations. Stanley has experience in acting for groups of companies, insolvency practitioners, and shareholders in a wide range of industries including that of payment processing, cryptocurrency, and media technology.

Contact Stanley Tan: stanley.tan@rajahtann.com





ICC FraudNet
Global Annual Report 2022

PART SIX

INSOLVENCY RELATED ISSUES

Using Receiverships to Investigate and Combat Fraud

Joe Wielebinski and Matthias Kleinsasser

Abstract

In this article, Joe Wielebinski and Matthias Kleinsasser of Winstead PC provide an overview of U.S. receivership law and discuss how this equitable remedy may be used to combat fraud alone, or in concert with other creditor remedies. The article lays out the basics of what a receivership is and what legal tools are available to a receiver charged with administering a receivership estate when fraudulent conduct is at issue. The article further discusses practical considerations for persons who suspect (but perhaps cannot confirm) they have been the victims of fraud and who wish to seek appointment of a receiver.

1. Introduction

Appointment of a receiver originated centuries ago in English courts of chancery under principles of equity. Broadly speaking, a receivership is an equitable remedy derived from common law under which a court appoints a person (the receiver) as an officer of the court to manage and protect property (the *res* or receivership estate, which often consists of a corporate entity and its assets), generally because the property is threatened by dissipation or diminution in value.¹ A receiver is usually granted extensive powers by the appointing court to manage assets, file claims, recover transferred property, and take other actions designed to preserve the receivership estate. For this reason, the appointment of a receiver is a flexible remedy that can be tailored to address specific circumstances. Since the appointment of a receiver usually results in displacing an entity's governing persons, however, courts generally require significant proof of fraudulent conduct, or, at a minimum, that an entity's or asset's value is seriously threatened, to grant this relief.

¹ The potential scope of the *res* is very broad. When a business entity is in receivership, the *res* will often include accounts receivable, real and personal property, causes of action, and intellectual property—in short, the entirety of the business's assets.

2. Basics of U.S. Federal and State Receiverships

- What is a receivership?

Receiverships are available under U.S. federal and state law, although the availability of the remedy, and the factors required to be satisfied to appoint a receiver, vary between U.S. jurisdictions.² For example, most U.S. jurisdictions permit a receiver to be appointed for fraudulent conduct on the part of the governing persons, particularly if those persons have fraudulently transferred assets or taken other actions that threaten the rights of creditors or equityholders.³ Appointment of a receiver is also a remedy commonly sought and obtained by government regulators when fraudulent conduct is suspected and/or the interests of investors are threatened—e.g., in proceedings brought by the U.S. Securities & Exchange Commission.⁴ The existence of fraud is generally not a requirement to appoint a receiver. When the entity is insolvent or in danger of insolvency and the business’s assets are threatened by a serious decline in value that would severely prejudice creditors, a court will often appoint a receiver regardless of whether fraud is suspected.⁵ Some U.S. jurisdictions have also enacted statutes allowing a receiver to be appointed over particular types of property, such as commercial real property.⁶ Moreover, the relevant statutes or the common law of many jurisdictions permits a receiver to be appointed for any reason justified by the rules of equity, thereby giving courts broad discretion in applying this equitable remedy.⁷ In addition, loan documents and other contracts frequently provide one party with the right to obtain the appointment of a receiver in its sole discretion, though courts are split as to whether such a contractual provision is enforceable.⁸

² See, e.g., Fed. R. Civ. P. 66 (stating that an action in federal court in which the appointment of a receiver is sought is governed by the Federal Rules of Civil Procedure); *Brill v. Harrington Invs. V. Vernon Savs. & Loan Ass’n*, 787 F. Supp. 250, 253 (D.D.C. 1992) (listing several factors to be considered in appointing a receiver, such as fraudulent conduct on the defendant’s part and imminent danger of property being lost, concealed, or diminished in value).

³ See, e.g., Tex. Civ. Prac. & Rem. Code §64.001(a)(1) (permitting appointment of a receiver in an action by a vendor to vacate a fraudulent purchase of property); *Brill*, 787 F. Supp. at 253 (listing fraudulent conduct on the defendant’s part as a factor to be considered in appointing a receiver).

⁴ See, e.g., *Securities and Exchange Commission v. Stanford International Bank, Ltd., et al.*, 3-09CV0298-N, in the U.S. District Court for the Northern District of Texas, Dallas Division (“Stanford Receivership”), filings available at <http://stanfordfinancialreceivership.com/>.

⁵ See, e.g., Tex. Civ. Prac. & Rem. Code § 64.001(a) (permitting a Texas court to appoint a receiver in multiple situations, including over an insolvent corporation or over a corporation facing imminent danger of insolvency).

⁶ See, e.g., Maryland Commercial Receivership Act, codified at Title 24, 2019 Maryland Code, available at <https://law.justia.com/codes/maryland/2019/commercial-law/title-24/>.

⁷ See, e.g., Tex. Civ. Prac. & Rem. Code § 64.001(a)(6) (allowing a receiver to be appointed for any reason justified by rules of equity).

⁸ See, e.g., *LNV Corp. v. Harrison Fam. Bus., LLC*, 132 F. Supp. 3d 683, 690-91 (D. Md. 2015) (reviewing split of authority over whether a receiver may be appointed under a contract).

The breadth of a receiver’s potential powers is perhaps the most significant aspect of this equitable remedy. The receiver’s powers are typically outlined in the court’s order appointing the receiver, meaning that courts frequently can tailor the scope of the receiver’s authority to the circumstances of the case. In general, most courts appointing a receiver tend to grant the receiver extensive powers unless the receiver’s powers are circumscribed by statute (e.g., because the receiver is appointed under a statute authorizing the appointment only for a specific purpose, such as foreclosing a lender’s lien on real property). This could include the power to sell assets, commence litigation and/or initiate a bankruptcy proceeding, often without additional approval of the appointing court.⁹ For most purposes, the receiver stands in the shoes of the entity in receivership and may act to protect the interests of any parties with an interest in the entity, such as creditors and shareholders.¹⁰ Under the law of most jurisdictions, the receiver generally has authority to sell property or take other actions with respect to a business that could have been taken by the entity’s management, so long as those actions are authorized by the court order appointing a receiver. For example, receivers are regularly authorized to marshal assets, collect rents, pursue claims belonging to the entity, and review and pay creditors’ claims. Usually, an order appointing a receivership will prohibit creditors of the receivership estate and other third parties from taking action against the receivership estate outside of the court-sanctioned claims submission process.¹¹ In doing so, the court effectively streamlines the process of liquidating or rehabilitating the receivership estate and ensures that similarly situated parties are treated fairly. Of course, the order is limited by the court’s jurisdiction, and enforcement of the order against third parties may require the intervention of foreign courts.

Typically, the receiver must execute an oath that he/she will perform their duties in good faith and must provide a receivership bond in an amount set by the court as security should the receiver fail to perform his/her duties in good faith.¹² Receivers are deemed fiduciaries in most jurisdictions and must avoid engaging in self-dealing

⁹ See, e.g., Tex. Civ. Prac. & Rem. Code §§ 64.031-64.034 (listing receiver’s power to bring lawsuits, take possession of property, and take similar actions).

¹⁰ See, e.g., *Reid v. United States*, 148 Fed. Cl. 503, 523 (2020) (receiver “steps into the shoes” of the entity in receivership and owes fiduciary duties to creditors). Although the receiver will act to benefit all stakeholders, most receiverships pay creditors before providing a return to equity, consistent with good corporate practice and U.S. bankruptcy law. In large receiverships with assets having value above the secured creditors’ debt, creditors are generally provided with notice of a bar date by which they must submit their claims. Claims that are timely filed and allowed are then paid pro rata from the receivership estate under an established priority scheme. If assets have been fraudulently transferred (such as in a Ponzi scheme) or otherwise need to be recovered, the claims administration process may take years to complete while fraudulent transfer litigation is ongoing.

¹¹ See, e.g., Amended Receivership Order, *Securities and Exchange Commission v. Stanford International Bank, Ltd., et al.*, 3-09CV0298-N, in the U.S. District Court for the Northern District of Texas, Dallas Division (“Stanford Receivership”), available at [Amended_Order_Appointing_Receiver.pdf](#) ([stanfordfinancialreceivership.com](#)) (prohibiting parties from enforcing liens, seizing assets, pursuing claims, and taking other actions against the Stanford International Bank receivership estate). (Accessed October 11, 2021).

¹² See, e.g., Tex. Civ. Prac. & Rem. Code §§ 64.022-64.023.

or other actions that place the receiver's own interests above those of stakeholders in the receivership estate, such as creditors and equityholders.

Once the receiver has been appointed and has provided the oath and bond, the receiver will usually begin evaluating the financial situation of the receivership estate by reviewing assets and liabilities. If fraud is suspected, the receiver will investigate whether fraudulent transfers or other improper dissipation of assets has occurred. Receivers are often required to provide periodic reports and/or accountings to the court and are almost always required to file a final accounting once the receivership estate has been fully administered (i.e., all claims have been paid or all receivership property has been liquidated). Once the estate has been administered, the court will enter an order discharging the receiver.

3. How Can a Receivership Uncover Fraudulent Conduct?

A party seeking appointment of a receiver must do so by filing an application with a court of appropriate jurisdiction (or, where allowed, by making a request for receiver in a complaint or other document filed to commence a lawsuit). Given that a receivership is a powerful equitable remedy that effectively displaces the governing persons of an entity, courts do not appoint a receiver lightly. Most of the time, the applicant must show fraudulent conduct or other bad behavior on the part of an entity's management. At a minimum, the applicant must show that the business's assets are in jeopardy of losing substantial value, thereby threatening the interests of creditors and equityholders. If a less drastic equitable remedy is available that can protect the interests of creditors or other stakeholders (e.g., a preliminary injunction, which merely preserves the *status quo* until a dispute can be resolved by trial), courts will usually decline to appoint a receiver. For this reason, receiverships are most commonly used when the interests of multiple parties are threatened (e.g., all creditors of a business), as opposed to in a two-party dispute, where an injunction may be sufficient.

Given that fraudulent conduct is almost always secretive in nature, an applicant who suspects that an entity's governing persons have engaged in fraudulent conduct may face an uphill battle in acquiring sufficient evidence to justify appointment of a receiver. An additional problem is that the applicant may not wish to tip off a fraudster that a court action is coming before it is filed, thereby provide the fraudster with a window to fraudulently transfer, or dissipate assets. This is of particular concern if the fraudster has the ability to easily transfer assets to a foreign jurisdiction, given the additional difficulties and cost inherent in recovering assets abroad. As 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.¹³

To the extent possible, it is best for a potential receivership applicant to conduct as much pre-suit investigation as possible prior to filing suit. This should include public record searches (e.g., prior court filings or lien searches), internet searches using a search engine, and review of social media accounts. In particular, social media searches frequently turn up information that can later be used in a lawsuit to uncover fraudulent conduct. The applicant may wish to consider hiring a private investigator. If the applicant already has access to a significant amount of financial information relating to a business, the applicant should consider hiring a forensic accountant to determine if funds have been fraudulently transferred or other suspicious circumstances are present. Some jurisdictions also permit pre-suit discovery (e.g., a pre-suit deposition under Texas Rule of Civil Procedure 202), although the benefits of formal pre-suit discovery when fraudulent conduct is possible are often outweighed by the risks inherent in tipping off a fraudster that litigation is being evaluated. In short, pre-suit investigation can be difficult, but a party should, at a minimum, conduct Internet searches and review social media postings.

As the U.S. permits liberal discovery once a lawsuit has been filed, uncovering fraudulent conduct becomes much easier once a lawsuit is pending. The problem, of course, is that merely filing a lawsuit does not prevent a fraudster from dissipating assets while it is pending without some kind of additional equitable relief in place, like a preliminary injunction or appointment of a receiver. Obtaining either of these types of equitable relief requires more than mere suspicion that fraudulent conduct has occurred. Frequently, the best course of action for a party that has sufficient evidentiary support to file a lawsuit, but not sufficient evidence to obtain a preliminary injunction or receiver, is to file suit and seek expedited discovery, which may be authorized by the court in most jurisdictions.¹⁴ The lawsuit should be accompanied by a request for appointment of a receiver, which the applicant can amend to add additional factual detail if expedited discovery is authorized. The applicant should also consider seeking issuance of a temporary restraining order—a type of temporary injunction that generally lasts only 14-30 days—to preserve the status quo while expedited discovery is conducted.¹⁵ Once sufficient information is obtained through expedited discovery to justify appointment of a receiver, the applicant can request a hearing date with the court.

¹³ 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/1900690.pdf> (Accessed October 11, 2021).

¹⁴ Under Federal Rule of Civil Procedure 11 and its state law equivalents, a litigant must ensure that allegations in the lawsuit have evidentiary support, or at least are likely to have evidentiary support after a reasonable inquiry.

¹⁵ Because of the short lifespan of this type of injunction, courts are more willing to grant a temporary restraining order than a preliminary injunction (which holds the status quo until trial).

Most receivership orders provide a receiver with expansive powers to conduct litigation discovery, obtain documents, and prosecute claims—particularly when fraud is suspected. Therefore, once a receiver has been appointed where fraudulent conduct is suspected, the receiver will usually move quickly to obtain further information. This will generally involve using traditional litigation discovery devices such as requests for production of documents and depositions. If the cost can be justified, a receiver will often employ a forensic accountant to facilitate the review and analysis of financial information.

4. What Causes of Action Are Available to a Receiver Once Fraud is Uncovered?

Generally, the receivership order will allow the receiver to prosecute any causes of action belonging to the receivership estate (i.e., any causes of action that otherwise belong to the entity placed into receivership). Below is a non-exhaustive list of some commonly pursued causes of action:

- **Fraudulent transfer claims:** Virtually every U.S. state has a well-developed body of law that allows creditors to recover fraudulent transfers of money and other property from transferees. These laws are typically codified in the Uniform Fraudulent Transfer Act (“UFTA”) or the Uniform Voidable Transaction Act (“UVTA”, which is effectively a successor statute to UFTA), depending upon which statute has been adopted by a state.¹⁶ Section 548 of the United States Bankruptcy Code also contains provisions similar to the UFTA and UVTA, but requires the commencement or pendency of a bankruptcy proceeding. Fraudulent transfer law allows for recovery of two types of transfers. The first type are transfers made with actual intent to hinder, delay, or defraud a creditor, referred to as actual fraudulent transfers.¹⁷ To determine whether actual intent to hinder, delay, or defraud exists on the part of the transferor, most courts look to a list of so-called “badges of fraud” to see if any are present, though the list is not exclusive.¹⁸ The second type of avoidable transfer is a constructively fraudulent transfer. This type of transfer does not require actual intent to hinder, delay, or defraud on the part of the transferor.¹⁹ Instead, the transfer must have been made in exchange for less than reasonably equivalent value and while the transferor was either insolvent, undercapitalized, or not paying its debts as

¹⁶ For example, California has adopted by UVTA, while Texas still uses the UFTA.

¹⁷ See, e.g., Tex Bus. & Com. Code § 24.005(a)(1). Strictly speaking, fraudulent intent on the part of the transferor is not required to bring this claim so long as the transfer was at least intended to hinder or delay a creditor’s right to collect from the transferor.

¹⁸ See, e.g., Tex. Bus. & Com. Code § 24.005(b).

¹⁹ For this reason, the Uniform Voidable Transaction Act dropped the word “fraudulent” from its title.

they become due.²⁰ Constructively fraudulent transfer law effectively protects creditors by limiting the extent to which a party with limited assets can transfer those assets for less than reasonably equivalent value. Although fraudulent transfer lawsuits are traditionally brought by creditors, a receiver is typically granted the authority to file such actions to recover assets for the benefit of all creditors of the receivership estate. The lawsuit may be filed against the initial transferee of the transferred property and any subject transferee.²¹ In the case of a subsequent transferee, however, a person who took the property in good faith and in exchange for value is immune from a fraudulent transfer suit.²²

- **Breach of fiduciary-duty claims:** Frequently, a receivership estate will possess claims for breach of fiduciary duty, most commonly against a corporate entity's current or former officers and directors. Under Delaware law, officers and directors owe duties of care, good faith, and loyalty to the entity.²³ Broadly speaking, these duties require governing persons to avoid conflicts of interest and take actions they believe are in the best interests of the entity after becoming reasonably informed about a particular issue. Most U.S. states impose similar fiduciary duties on governing persons, although the extent of those duties and the exceptions to them can vary considerably among jurisdictions. Although many breaches of fiduciary duty do not involve fraud, fraud committed by a governing person with respect to an entity will generally constitute a breach of fiduciary duty. For example, a chief financial officer who falsifies company financials to procure additional investments has likely not only engaged in securities fraud, but also breached their fiduciary duties. A common remedy for breach of fiduciary duty is disgorgement of ill-gotten gains (e.g., profits) obtained as a result of the breach.
- **Restitution/unjust enrichment:** A third type of relief frequently sought by receivers is recovery of property or funds obtained unjustly, often referred to as unjust enrichment. Different jurisdictions have various names for causes of action based on unjust enrichment (e.g., quantum meruit or money-had-and-received).²⁴ Courts sometimes award relief based on restitutionary theories when a party has been unjustly enriched but, for whatever reason, the elements of a cause of action under contract or tort law cannot be

²⁰ See, e.g., Tex. Bus. & Com. Code §§ 24.005(a)(2), 24.006(a).

²¹ See, e.g., Tex. Bus. & Com. Code § 24.009(b).

²² *Id.*

²³ See *Stone v. Ritter*, 911 A.2d 362, 370 (Del. 2006) (listing fiduciary duties and noting that the duty of good faith is effectively a subsidiary duty of the duty of loyalty). . Traditionally, Delaware law is the most highly developed corporate law in the United States, due to the number of companies incorporated there.

²⁴ See, e.g., *Hill v. Shamoun & Norman LLP*, 544 S.W.3d 724, 732-33 (Tex. 2018) (discussing elements of quantum meruit claim under Texas law); *Plains Explor. & Prod. Co. v. Torch Energy Advisors Inc.*, 473 S.W.3d 296, 302 n.4 (Tex. 2015) (discussing money-had-and-received claim under Texas law).

established. Therefore, a restitution or unjust enrichment claim is rarely the only claim asserted by a receiver, but is often included in the complaint.

While a receivership offers many advantages to a victim of fraud, it is not perfect and has some disadvantages and drawbacks. First, a state court, unlike a bankruptcy court, may not have significant experience with complex fraud schemes, fraudulent transfer litigation or receiverships. Second, the court selects the receiver (often based on the recommendation of the plaintiff), but the court can decide to appoint someone else. That person may not have the necessary experience or manpower to handle the task. Third, a receivership is not cost free and can be expensive. Typically, receivers are paid from the assets of the estate but if there are no unencumbered assets or assets with equity value above the secured debt, the plaintiff will need to cover the costs, which can be significant. Finally, to frustrate the appointment of a receiver, the fraudster could commence a bankruptcy proceeding, which will stay any action to appoint a receiver and could displace any receiver already appointed. Of course, the filing of a bankruptcy by the fraudster may be a net positive for the impacted creditor for a variety of reasons beyond the scope of this article. These drawbacks and disadvantages, while not exhaustive, must be evaluated in determining whether a receivership is the best option available to an aggrieved creditor.

5. Conclusion

When faced with a company engaged in fraud or the dissipation of assets, creditors have to be prepared to use any legal mechanisms at their disposal. Receivership is one such mechanism and it provides numerous advantages discussed herein. However, it is not a perfect mechanism and has some drawbacks that must be considered. Nevertheless, the ability to have a court appoint an experienced third party as an officer of the court with broad powers to stop bad acts, preserve threatened or deteriorating assets, investigate the underlying facts and pursue appropriate claims for recovery is an important weapon and one that has proven effective in many situations involving fraud.

About the Authors



Joe Wielebinski, Shareholder, 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 litigations.

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 and Turnaround Management Association.

Contact Joe Wielebinski: T. (214) 745-5210; E. jwielebinski@winstead.com



Matthias Kleinsasser, Of Counsel, 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 suite, 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, as well as represented debtors, creditors, and trustees in virtually all aspects of business bankruptcy proceedings, including contested asset sales and debtor-in-possession financing.

Contact Matthias: T. (817) 420-8281; E. mkleinsasser@winstead.com

Recognition of Foreign Insolvencies in Panama

Donald Andersson Sáez Samaniego

Abstract

In this article, Donald Andersson Sáez Samaniego of MDU LEGAL Law Firm, examines the aims, requirements and effects of the recognition of foreign insolvencies in the Republic of Panama, according to Law No. 12/2016, which regulates insolvency matters in Panama and became effective on January of 2017. Based on professional experience and academic research, the author presents an overview of the currently applicable legal provisions and Panamanian court procedures relative to foreign insolvencies.

1. Jurisdiction of the Courts of Panama on matters related to recognition of foreign insolvencies

Jurisdiction to decide the recognition of foreign insolvencies in Panama lies with the Fourth Superior Court of the First Judicial District of Panama. This was created by Law 12 of March 19, 2016, which established a new legal regime for insolvency matters (the “Law” or “Insolvency Law”).¹ However, this court specialized in insolvency matters has not been implemented due to a “lack of economic budget”, as stated by Panama’s Judicial Branch.²

Nevertheless, the Law provides a transitory solution to address this situation. That solution is found in article 262 of the Law. This grants the existing circuit courts the provisional power to hear the recognition matters, first starting in 2017 and until the insolvency courts and the Fourth Superior Courts begin operations.

The delay in implementing the creation of the new Superior Court also impacts its jurisdiction to act as a court of appeals for insolvency matters. Initially these functions were handled by the existing Superior Courts in the district corresponding to each trial court.

¹Available at the Official Gazette’s website, https://www.gacetaoficial.gob.pa/pdfTemp/28036_B/56238.pdf, [accessed August 11, 2021].

² Panama’s Judicial Branch is one of its three government branches. Its website is located at: <https://www.organojudicial.gob.pa/>, [accessed August 11, 2021].

Recently, following the enactment and implementation of Law No. 231 of June 2021, a paragraph was added to article 262 of the Insolvency Law provisionally granting appellate jurisdiction on insolvencies to the Third Superior Court of the First Judicial District ³over those appeals which the Insolvency Law had slated to be heard by the Fourth Superior Court which is still not operative. In other words, starting on the promulgation of Law No. 231, the Third Superior Court has provisionally taken jurisdiction to hear challenges arising from insolvency proceedings currently heard by the circuit courts. It is worth noting that the first group of cases to be heard by the Third Superior Courts were assigned on July 30, 2021.⁴

2. Reasons for the recognition of cross border insolvencies⁵:

Prior to dealing with the recognition of foreign insolvencies in Panama, it is worthwhile discussing the importance or purpose served by such recognition. Such purpose may be summarized in five fundamental objectives, each being significantly important.

- 2.1. The first aspect deals with the desire to encourage cooperation between the Republic of Panama and foreign states regarding insolvencies. It is no coincidence because the Law seeks to avoid pending litigation claims and duplicity of proceedings which may result in a multiplicity of rulings and even contradictory decisions.
- 2.2. Another important aspect to consider in the recognition aims to provide additional legal protections for international trade and investment. Clearly, any investor wants to know that their investments are secure and that their rights will be respected, independently of the financial situation faced and the obligations towards creditors.
- 2.3. Related to this, a third objective concerns the fair and efficient management of the cross-border proceedings to allow the protection of all creditors, interested parties and even the debtors themselves.

³ Republic of Panama has been divided in four Judicial Districts for a better organization. The First Judicial District include provinces of Panama, Colon, Darien and regions of Guna Yala, Madugandi, Wargandi, Embera Wounaan. First Judicial District has the Third Superior Court, who hold appellate jurisdiction regarding matters like monopolistic practices; consumer law, intellectual property controversies and others, and more recently in insolvency matters.

⁴ This link directs us to a news article published by the Judicial Branch regarding the first assignment of insolvency matters to the Third Superior Court. <https://www.organojudicial.gob.pa/noticias/se-realiza-primer-reparto-de-procesos-concursales-de-insolvencia-en-el-tercer-tribunal-superior-de-justicia>, [accessed August 12, 2021].

- 2.4. In this same line of thought, the fourth justification for the recognition of foreign insolvency is aimed at protecting the debtor's assets and their conservation to optimize their value to satisfy the creditors. Obviously, inasmuch as the assets do not deteriorate but rather be optimized or improve, these could be subject to judicial auction, and their monetary value would be useful to compensate a greater number of creditors.
- 2.5. The final point relates to seeking coordination for the reorganization of a company facing financial difficulties to protect capital and preserve jobs.

3. Requirements which must be met for the grant of recognition of a foreign proceeding and types of recognition

The recognition of a foreign insolvency in Panama is premised on the fulfilment of certain requirements. For example, it is necessary to enclose an authentic copy of the order which initiates the foreign proceeding, and which designates the foreign representative in the proceeding. If this is not possible for any reason, the Law allows for the presentation of a certification by the foreign court, accrediting the existence of the insolvency and the designation of the foreign representative. If this is still not possible, the petitioner may rely on other lawful evidence if it does not contravene the local laws.

Additionally, it is indispensable to include a statement mentioning all the foreign proceedings filed against the debtor about which the representative has knowledge. All foreign documents must be duly legalized for them to be valid in Panama either through the apostille or with a consular representative. Once this documentation has been submitted, the competent court must look at it and if found to be in conformity, it must issue an order accepting the recognition, as long as the foreign proceeding is of a similar nature or the equivalent to the Panamanian insolvency proceedings. The foreign representative must be accredited in the foreign court to manage the reorganization or liquidation of the debtor's business, or to act as a foreign representative.

Recognitions may be granted as a 'principal foreign proceeding' when it is being handled in the debtor's principal place of business, or as a 'not principal foreign proceeding', if the debtor has a permanent business establishment in the foreign jurisdiction. The difference between one and the other is that in the first one there are measures which are ordered automatically by operation of the Law; while the second one requires a request by the movant and are subject to the judge's discretion.

4. The Court may adopt provisional measures as part of a request for recognition

There are provisional measures available starting with the request for recognition upon application by the petitioner. The court may issue such provisional or cautionary measures immediately upon recognition among which is the stay of all foreclosures against the assets of the insolvent debtor.

Another such measure is granting the foreign representative receivership powers over the debtor's assets located in Panama, as well as an asset freeze. Giving testimony and presentation of evidence is also available as a provisional measure, as well as disclosure orders related to the debtor's assets, businesses, rights and obligations, without prejudice to any other measures compatible with the forum's laws.

Following recognition of a foreign insolvency as a 'principal proceeding' the debtor's assets are protected from foreclosures outside the insolvency recognition and all ongoing cases are automatically stayed. Asset transfers are suspended as is the right to lien or dispose of the debtor's assets upon risk of being set aside.

There are other measures aimed at preserving the debtor's assets and to submit to a universal proceeding all claims against the debtor whether or not they are pending at the time of the recognition. Such measures include a stay on new filings against the debtor and the stay of ongoing actions, protection of its assets to prevent dissipation. All other remedies available under the Insolvency Law are also available following the recognition.

Conclusion

In short, the recognition of foreign insolvencies in Panama are very useful, because grant to the debtors and creditors the legal security that there will not subject to multiplicity of process or contradictory rulings regarding the same topic. Moreover, an important tip is that, with a foreign recognition in Panama, the debtor's assets located in the territory would be subject to precautionary measures in order to assure they are not transfer to other person/owner, and so, these hold available in favor of the creditors in order to collect or compensate his pendant credits.

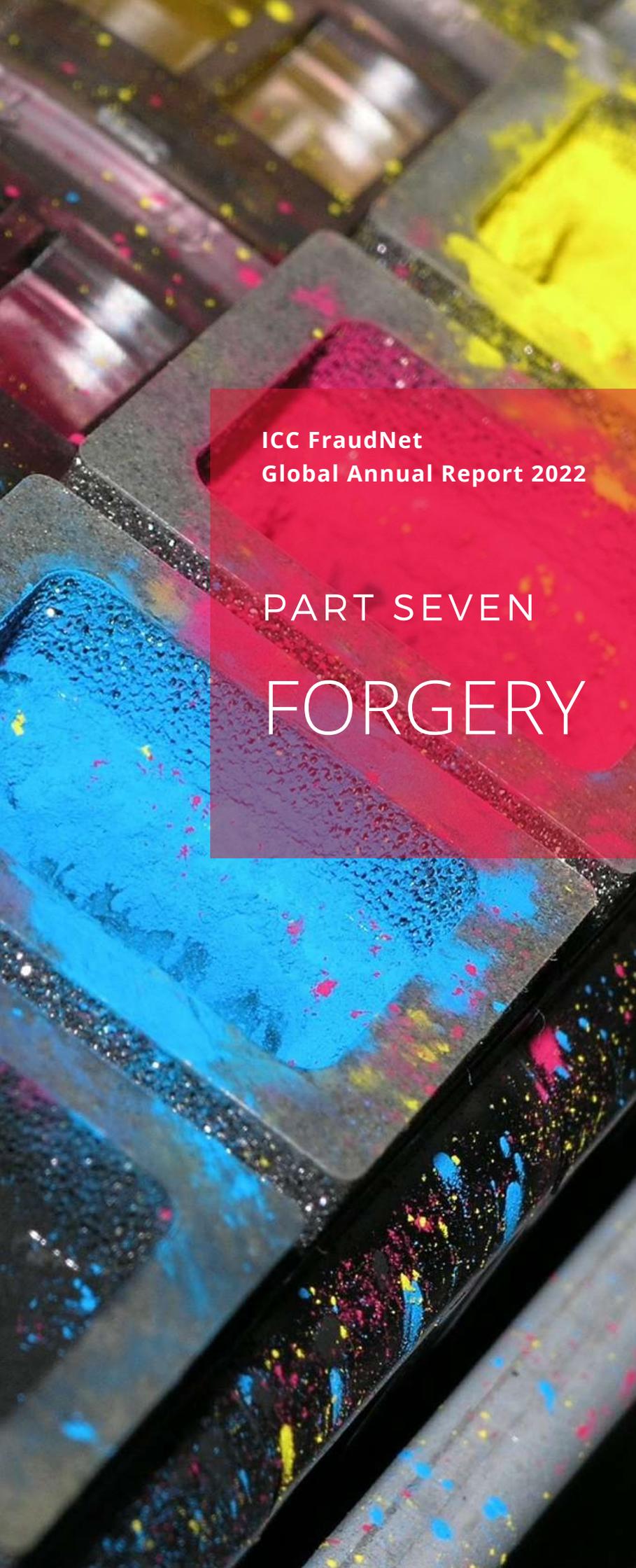
About the Author



Donald Andersson Sáez Samaniego is an academic and attorney admitted by the Supreme Court of the Republic of Panama. He holds a Bachelor of Laws and Political Sciences with high honors (Cum Laude Charter) from the University of Panama, and a Master of Laws (International Law, emphasis on Private International Law) at the Complutense University of Madrid, and a Postgraduate Degree in Higher Teaching at the University of the Isthmus. Also, he has a Bachelor in criminalistic and forensics sciences.

He is an Associate Lawyer at MDU Legal, and his practice focuses on International Law; Civil law; Commercial law; Insolvency/Bankruptcy (national and cross-border); Corporate law; Assets Recovery and Litigation. Mr. Sáez Samaniego, as expert in Panamanian Law, has served clients in numerous jurisdictions including Switzerland; England; Austria; Singapore; Peru, US, BVI; Brazil; Costa Rica. He has advised several multinational companies.

Contact Donald Andersson Sáez Samaniego: T. +(507): 263-0604; E. dsaez.mdu@gmail.com; A. Suite 6C, ADR Building, Samuel Lewis Avenue and 58 street, Obarrio, Panama, Republic of Panama.



ICC FraudNet
Global Annual Report 2022

PART SEVEN
FORGERY

Wine Fraud in Spain: Has Over-Regulation of the Industry Led to Self-Sabotage?

Héctor Sbert Ph.D.

Abstract

When it comes to wine fraud, what often springs to mind are characters such as Rudy Kurniawan,¹ who produce counterfeit versions of prestigious wines. As the perpetrator in one of the most high-profile wine fraud cases in history, Kurniawan was deported from the US earlier this year after being convicted in 2013 of conning wealthy wine collectors out of millions of dollars. However, many fraudsters also exist within the wine industry itself. In this article, Dr Héctor Sbert, Partner at ECIJA, explores some of the key factors behind an apparent rising tide of wine fraud, with a particular focus on Spain. This type of fraud is not surprising because France, Italy and Spain concentrate between half and two-thirds of the world's wine production. In doing so, Dr Sbert considers the future of the industry and some examples of institutional initiatives designed combat this type of criminality.

Rotten on the Inside

Interestingly, there's a concentration of wine fraud activity in areas with '*Protected Designation of Origin*' or 'DOP' status. This means where regulatory bodies have been created to certify the quality of these valuable wines and protect their producers. Some wine industry insiders have been discovered breaking various rules surrounding production techniques, the surpassing of quotas, and mislabelling of wines.

What we want to consider here is whether the over-regulation of wine, particularly in those areas controlled by DOPs, has contributed to an increase in fraudulent activity. Currently, the European Commission estimates the economic impact of such crimes to be €1.3 billion a year² (which is 3.3% of total annual wine sales) across the

¹ See reports at Decanter.com, <https://www.decanter.com/tag/rudy-kurniawan/> (last visit July 27, 2021).

² See European Commission, "Wine fraud - EU database for chemical analysis to protect the identity, origin and quality of wines (implementing rules)", available at <https://ec.europa.eu/info/law/better->

region. Therefore, let's consider here some of the DOP rules that may have inadvertently resulted in the incentivization of deception for producers and various other wine professionals.

What Makes a DOP-Certified Wine?

According to DOP criteria, certain aspects of wine production must meet controls set by the regulators for their respective origin areas. These include the types of grapes that can be used, the geographical area, the quantity of wine that can be produced (production quotas), requirements around growing and production techniques, laboratory analysis of the wines, and blind tastings by experts.

Should a wine pass on all these fronts then it can, in theory, be verified and certified with a stamp of identification from the DOP. These usually take the form of a small label on the back of the wine bottle that is printed using banknote techniques. This translates to value in the premium certain markets are willing to pay for regulated wines as a hallmark of quality, specially internationally. These premiums come on top of the price control implicitly derived from production quotas that regulation imposes on wine manufacturers. Therefore, DOP-certifications not only benefits consumers (ensuring a certain degree of quality), but also producers, ensuring there won't be price fluctuations due to excess production. On the other hand, production quotas become problematic when they are exceeded, forcing producers to find "other ways" to sell their product, thus leading to sometimes irregular behaviours that, in most cases, can be considered fraudulent.

A Focus on Spain

Spain makes an interesting case study when it comes to wine fraud as Spanish wine is among the most falsified in Europe. In fact, Rioja, as the most valuable wine of Spanish origin and with approximately 300 millions of litres sold annually, is said to be the most imitated variety of wine across the continent. This has led to many bottles of wine being sold as Rioja in restaurants, stores, and online when they are not the real deal.

[regulation/have-your-say/initiatives/12729-Wine-fraud-EU-database-for-chemical-analysis-to-protect-the-identity-origin-and-quality-of-wines-implementing-rules-_en](https://www.iccfraudnet.org/regulation/have-your-say/initiatives/12729-Wine-fraud-EU-database-for-chemical-analysis-to-protect-the-identity-origin-and-quality-of-wines-implementing-rules-_en) (accessed on July 27, 2021).

Labelling Fraud

In 2016, an investigation by the Spanish Guardia Civil uncovered fraud on a global scale, where Rioja, that was not in fact Rioja, was mislabelled and sold nationally and internationally. The fake wines bearing the brands *La Bella Fernanda* and *6 Sombreros* were available to buy in Spain, Canada, and the United States, with prices ranging between 13.50 and 32.95 euros per bottle.

Following the discovery during a routine inspection of a restaurant in Barcelona, the national guard was alerted to the fake Rioja. This resulted in the raiding of premises in the La Rioja region where they uncovered 50,000 fraudulent labels and 1,400 bottles of wine, along with thousands of corks, plastic toppers, and machinery. A DOP-affiliated wine producer from La Rioja and a wine distributor from Catalonia were detained on the grounds of selling wine as Rioja when it did not have the necessary certification label or security seal. Incredibly, they had been in business for 10 years prior to the investigation.

Where did the wine come from?

The Guardia Civil hypothesized that the wine had either originated from excess production by the producer in question that was above the permitted DOP limit, or that the wine had perhaps come from outside the DOP area of Rioja. However, the regulatory board for Rioja (*Consejo Regulador de la Denominación de Origen Calificada Rioja*) claimed that despite the producer being one of those with DOP certification, this fraudulent DOP-branded wine had, according to their analyses, originated from another area. This meant that the fraud was outside the realm of their responsibility, and perhaps their interest.

The Dark Side of Production Quotas

Multiple such cases of labelling fraud have been seen in Spain, which could arguably be the result of production quotas imposed by DOP regulatory boards to control the price of their wine. Producers with a surplus of wine may attempt to distribute the excess bottles using fake or illegal labels instead of risking it being unsold or having to sell it for less than DOP value prices. They may also oversell their quotas in terms of the amount of wine actually sold, versus the amount that is declared to the DOP regulator.

An example of this is the ongoing case of wine fraud that arose in the DOP Valdepeñas region in 2020. This investigation, currently with Spain's national court,

has seen major DOP-certified players accused of mislabelling their wine as *Crianza*, *Reserva*, or *Gran Reserva*, but without the necessary conditions for these vintage classifications being upheld. This classification of wines in reference to the time of maturation and ageing given to them in the winery is typical of Spain and, therefore, we will only find it in wines of Spanish origin.³

It's been said that part of the reason why they were able to take advantage of this is due to the generic labelling requirements of DOP Valdepeñas wines. What's more, one of the defendants has accused another producer of infiltrating and influencing the region's DOP activity via its Vice President. They complain that the Valdepeñas regulatory body is corrupt, is operating with a lack of transparency and management structure, and without proper safeguards in place.⁴

A Private Club

Some wine producers are not able to benefit from DOP credentials, despite using the same grapes in the same regions as those who come under its protection. This means that if a regulatory board has registered the use of the place name on labelling then other producers in the region are not permitted to do so in their marketing.

Such opacity of toponymy was shown in the case of a small organic family winery in Catalonia, which was recently fined⁵ for putting the location of their winery on the label as they are not affiliated with the local DOP. Excluded producers have likened DOP regulators to private members clubs looking out for their own economic interests.

Where Does This Leave Consumers?

Buyers who are not aware of labelling standards are more vulnerable when it comes to their potential for purchasing fake DOP-certified wine. They may not know to check the back of the bottle or how to spot other signs that a wine is not genuine.

³ Thus, speaking only of red wines, only those with a minimum total ageing of 24 months, of which at least 6 months must be in oak barrels, fall into the *Crianza* category. For the *Reserva* category, the total ageing period for red wines must be at least 36 months, with a minimum of 12 months in barrels. Finally, in the case of red wines, the *Gran Reserva* category would be for wines with a minimum total maturation time of 60 months. And these wines should spend at least 18 of those 60 months in oak barrels.

⁴ See reports at the Spanish press at <https://www.eleconomista.es/empresas-finanzas/noticias/10629477/06/20/Valdepenas-admite-un-fraude-en-casi-la-mitad-de-los-vinos-de-crianza-vendidos.html> (last visit 29 October 2021).

⁵ According to reports released by Spanish national television, available at <https://www.rtve.es/noticias/20210613/denominacion-origen-desata-guerra-varias-bodegas-espanolas/2102101.shtml>, (last visit 27 July 2021).

In general, DOP criteria in Spain dictates that wine must display the small label of certification on the back of the bottle, however, the producer or distributor can put whatever they like on the front label.

How Do You Solve a Problem Like the DOP?

So, to whom will it fall to counter this rising tide of Spanish wine fraud? It does appear, as a result of recent action, that authorities are taking the issue increasingly seriously. Spain's Guardia Civil has begun conducting training with three DOP-certified wine producers in the Tarragona area of Catalonia on how to combat wine fraud. The scheme was organized following commitments from the General Director of the Civil Guard and the President of the Spanish Conference of Wine Regulatory Councils.

There are multiple objectives of this collaboration. They range from increasing food safety through better prevention and investigation of illegal activities, improving the protection of consumers, and supporting the legitimate interests of companies in the wine sector - both nationally and internationally. Furthermore, the scheme hopes to restore lost credibility to the Protected Designation of Origin status and thus generate confidence from consumers that would enable further development in the Spanish agri-food sector.

DOP Fraud Across the Board

Of course, it's not just wine that is vulnerable to this type of crime. Other valuable certified industries also see their fair share of dirty tricks. One example of this is the Great Canadian Maple Syrup Heist of 2011, which saw the Federation of Quebec Maple Syrup Producers accused of being involved in the theft of 3,000 tonnes of the region's maple syrup that was being stored in their facility because of their desire to control the global supply and therefore the prices of their syrup.

Conclusion and Outlook

The bureaucracy, corruption, or inaction of certain regulatory bodies has hurt the integrity of Spanish DOP-certified wine, alongside other wines and other products around the world. Surely, we need to see a shakeup to ensure that the DOP stamp protects both the consumer and the producer going forward. This transformation to a transparent, fair, and functional framework, rather than a pervasive 'old boy'

network, would enable the wine industry to thrive, for growers to be paid better, and for smaller producers to be valued without such reliance on big industry. The fresh training program underway in Catalonia seems at least to be a step in the right direction. Also, suppliers, collectors, wine investors, as well as international exporters, distributors and consumers (probably the most vulnerable subjects in the supply chain) should be made aware of the shortcomings of the current regulatory framework and be given the proper instruments to combat such unacceptable behaviours, also through proper international cooperation channels.

About the Author



Héctor Sbert is a Litigation and Insolvency Partner at ECIJA Barcelona. Héctor has more than 20 years of experience advising national and international clients from all sectors in the field of litigation and insolvency law, and has been recognized by prestigious international rankings like Best Lawyers and Who's Who Legal in his practice areas.

Héctor is an expert in international commercial litigation and arbitration, in particular in the enforcement of national and foreign judgments, asset tracing and recovery, civil and commercial fraud and contentious insolvency. He is also the representative for Spain of ICC FraudNet, a global network of lawyers that, under the auspices of the International Chamber of Commerce (ICC), brings together the leading international specialists in asset tracing & recovery.

He is a Member of the London Chartered Institute of Arbitrators (MCI Arb.) and a Registered Mediator at the Ministry of Justice. Sbert holds a Ph.D. in Law from the Pompeu Fabra University and an Executive MBA from IESE. In addition, he has been Member of the Deputy of the Governing Board of the Barcelona Bar Association (ICAB) and Chair of the Bar's Ethics Commission. Héctor speaks Spanish, Catalan, English, French, German and Italian.

Contact Héctor Sbert: T. +34 933 808 255; E. hsbert@ecija.com

The Honest Forger and the Importance of Crying Foul: Insights on Forgery in English Law

Hugh Norbury QC and Dan McCourt Fritz

Abstract

As a matter of English law, are there acts that are so inherently unacceptable that they should be adjudged 'dishonest' by the standards of ordinary decent people even where they are prompted by reputable professional advice? In *Re Infund LLP* - in respect of which an appeal to the UK Supreme Court was discontinued prior to being heard in October 2021 - that question was answered in the affirmative at first instance. The authors challenge that conclusion, arguing that a proper application of the two-stage test formulated in *Ivey v Genting Casinos* should have resulted in the claimant in *Infund* being acquitted of dishonesty. They then go on to consider other recent related developments in English law.

Is it possible to 'forge' a document in a way that is not dishonest in the sense explained by the United Kingdom Supreme Court in *Ivey v Genting Casinos (UK) Ltd* [2017] UKSC 67? Following *Ivey*, when dishonesty is in question a fact-finding tribunal applying English law undertakes a two-stage inquiry:

- (1) First, it ascertains (subjectively) the actual state of the relevant individual's knowledge or belief as to the facts. The reasonableness of their professed belief is a matter of evidence going to whether it was genuinely held, but there is no additional requirement that the belief must be reasonable;
- (2) Once the actual state of the relevant individual's knowledge or belief as to facts is established, the question of whether their conduct was dishonest is determined by applying the (objective) standards of ordinary decent people.

There is no requirement that the individual must appreciate (subjectively) that their conduct was dishonest by those standards.

The case of *Re Infund LLP* - an appeal in which was due to be heard by the United Kingdom Supreme Court in October 2021 but was ultimately withdrawn - raised the interesting question of whether there are acts that are so inherently unacceptable that they should be adjudged 'dishonest' by the standards of ordinary decent people even where they are prompted by specialist professional advice from a reputable person or firm.

In *Infund*, a Mexican layperson (Mr García) wished to have an English LLP restored to the register. He obtained advice from a reputable firm of English solicitors ("Harris Cartier") as to how he should do so. That firm expressly advised Mr García that (1) it was permissible for Mr García to sign the necessary forms as a "*former member*" of the LLP even though he had never in fact been a member (but was only seeking to be appointed as a member prospectively), and (2) the form appointing Mr García should be backdated prior to 13 June 2007 to enable him to approve annual returns for the LLP that were produced on that date.

Mr García did not accept this advice unquestioningly. To the contrary: his Mexican lawyer asked whether the words "*prospective member*" could be included under each signature by Mr García in order to avoid any misrepresentation to Companies House (the government agency responsible for maintaining records of companies and LLPs). Harris Cartier responded restating their earlier advice, saying that it was in part based upon what the restoration team at Companies House itself had told them. They went further, telling Mr García that inserting the words "*prospective member*" anywhere in the forms would invalidate them.

Importantly, the claimants did not allege that any of Harris Cartier, Mr García's Mexican lawyer, or indeed the corporate and trust advisor that assisted Mr García with his application for administrative restoration had acted dishonestly. They therefore had to be presumed honest. The Court was thus required to proceed on the basis that Mr García had made the application in reliance upon advice from honest solicitors with the assistance of an honest corporate advisor and an honest Mexican lawyer. In other words, if Mr García acted dishonestly, he did so alone and despite the honesty of his advisors and representatives.

Having received advice from honest English solicitors in relation to technical and arcane matters of English company law, challenged that advice, and had it confirmed, Mr García followed it. It is difficult to imagine that an ordinary decent 'person on the street' would consider him to have acted dishonestly in doing so; indeed, the fact of Mr García challenging the advice demonstrates that far from intending to mislead Companies House, he was anxious not to do so.

The trial judge (Henry Carr J, now sadly deceased) nevertheless concluded that Mr García had acted dishonestly in completing the relevant forms in accordance with Harris Cartier’s advice. He posed the question: “*Would an ordinary decent person accept legal advice that a document should be forged?*”¹ The judge answered that question in the negative, saying that “*Mr García was advised to tell lies on forms submitted to the Registrar to achieve an administrative restoration. An honest person would not have done this.*”

With the greatest respect to the judge, the characterisation of Harris Cartier’s advice as “*advice to tell lies*” was unfair. It made inevitable his conclusion that Mr García had acted dishonestly in following Harris Cartier’s advice: by definition, honest people do not ‘lie’. Similarly, while backdating documents may technically constitute ‘forgery’ as a matter of English law, describing Harris Cartier’s advice pejoratively as “*advice that a document should be forged*” loaded the inquiry against Mr García.

If Henry Carr J had instead framed the question: “*Would an ordinary decent layperson accept legal advice as to how to complete technical administrative forms in a foreign jurisdiction?*”, we suggest that he would have been bound to acquit Mr García of dishonesty.

The Court of Appeal granted permission to appeal against the order of Henry Carr J on (amongst other bases) the basis that the trial judge had been wrong to hold that Mr García had acted dishonestly in making the application for administrative restoration. Regrettably, it did not decide that question, upholding the order of the trial judge on different grounds so that “*it matters not whether the presentation of the material to the Registrar was or was not fraudulent and dishonest as found by the judge*”.²

In our view, Henry Carr J was wrong to hold that Mr García acted dishonestly in making the application for administrative restoration. However, the facts that he reached the conclusion that he did, and that the Court of Appeal did not take the opportunity to disapprove it, provide a salutary warning. In English law, there may be no room for ‘honest’ backdating or other knowing misstatement. Such conduct could be so offensive to judicial sensibilities that it will invariably be ruled ‘dishonest’,³ no matter what the person on the street might think.

A related issue of general importance arose in *Infund*, and in the ongoing *Taylor v Van Dutch* litigation.

¹ The first instance judgment [2018] EWHC 1306 (Ch) at [95].

² Court of Appeal judgment [2019] EWCA Civ 1673 at [52].

³ First instance judgment at [155].

In *Infund*, the claimants contended that Mr García had forged a mandate dated 15 June 2003 (the “Mandate”). The claimants did not plead any allegation that the mandate was forged, but shortly before the trial served a notice to prove the Mandate under CPR 32.19.⁴

It is a sacrosanct principle of English law that allegations of dishonesty must be distinctly pleaded and particularised: see e.g. *Three Rivers District Council v Governor and Company of the Bank of England* [2001] UKHL 16 per Lord Millett at [186].

In *Infund* Henry Carr J said: “*If the Claimants had attempted to introduce an unpleaded and unparticularised allegation of forgery without notice, I would not have allowed them to rely upon it.*” However, he held that sufficient notice of the allegation of forgery was provided by the notice to prove the Mandate, saying that from the date of the notice “*Mr García could have been in no doubt that the Claimants were challenging the authenticity of the [Mandate]... [and] in the unusual circumstances of this case, further particularisation was unnecessary.*” On that basis, the learned judge concluded that the claimants were entitled to rely upon the forgery of the Mandate in support of their claim for rectification of the Register of Companies.⁵

In our view, this was (again) a somewhat surprising decision. Serving a notice to prove a document does not involve a specific allegation of forgery or fraud, let alone an allegation of sufficient particularity to comply with professional and procedural requirements for making such an allegation. In addition, Mr García arguably should have been given a greater opportunity to respond to the unspoken allegation of fraud in evidence.

Be that as it may, in an appropriate case those litigating in England might consider using a notice under CPR 32.19 as a tool for exerting pressure on the other side, and (following *Infund*) as a means of paving the way for advancing an unpleaded allegation of dishonesty.

The other side of the coin came to light in *Taylor v Van Dutch*. In that case, the claimant’s failure to serve a notice under CPR 32.19 (or plead any allegations of dishonesty) debarred him from cross-examining witnesses on the basis that documents had been forged. That drove the claimant to disavow altogether any allegation of dishonesty, forcing him to argue for a conspiracy to make negligent (rather than fraudulent) misrepresentations - a logical impossibility. The judge’s reasons for rejecting that claim in conspiracy warrant careful reading.⁶

⁴ Of the English Civil Procedure Rules 1998.

⁵ First instance judgment at [156].

⁶ [2019] EWHC 1951 (Ch) at [301]-[306].

Taylor v Van Dutch emphasises the importance of making any allegation of dishonesty at the earliest stage and in the clearest terms possible. The English courts will not permit litigants to ‘wound without striking’, and - notwithstanding the approach to the CPR 32.19 notice in *Infund* - the only safe course is to plead and particularise any allegations of fraud or forgery that are sought to be advanced.

An interesting postscript to the first instance decision in *Taylor v Van Dutch* (in respect of which the claimant brought an unsuccessful appeal⁷) concerns the claimant’s subsequent claim that the judgment referred to above had been obtained by fraud on the part of certain defendants. In support of that claim, the claimant sought a proprietary injunction which, if granted, would have stayed his obligation to pay the costs of his failed claim.

The claimant did so on the ground that moneys paid pursuant to a fraudulently obtained costs order were analogous to moneys stolen by a thief, and therefore would be recoverable and traceable in equity (as Lord Browne-Wilkinson explained in *Westdeutsche Landesbank v Islington London Borough Council*⁸ stolen moneys would be).

Falk J rejected that submission on the basis that the costs order would be valid unless and until it was set aside, so that “*Any money paid pursuant to it would transfer both legally and beneficially to the payee*”.⁹ The claimant would be paying the defendants’ costs “*because he is compelled by a court order, and not because someone has wrongly taken his property without his consent*”;¹⁰ and an order of the court is not properly characterised as ‘voidable’.¹¹

⁷ *Taylor v Rhino Overseas Inc* [2020] EWCA Civ 353.

⁸ [1996] AC 669 at 716C-D.

⁹ *Taylor v Khodabakhsh* [2021] EWCH 655 (Ch) at [89].

¹⁰ *Ibid.* at [92].

¹¹ *Ibid.* at [94].

About the Authors

Hugh Norbury QC has a broad commercial and chancery practice, with a particular emphasis on cases involving fraud, breach of fiduciary duty and confidential information. He is highly recommended by the leading directories in all his principal practice areas.



He has been involved in some of the most significant fraud cases of recent years. He is currently co-leading a US\$800m bribery claim against the former Director General of the Kuwaiti State Pension and Social Security Fund and has been acting since late 2019 in *Vale v Steinmetz*, a £1 billion-plus claim relating to a mining joint venture in Guinea. He is also currently acting in *Ballacorey Wheat v Brown & ors*, a fraud claim commenced in 2019 in the Isle of Man (relating to asset management) and in *Athene v Siddiqui & ors*, a claim commenced in Bermuda involving allegations of breach of fiduciary duty and dishonest assistance relating to confidential information in insurance and private equity.

Contact Hugh Norbury QC: clerks@serlecourt.co.uk



Dan McCourt Fritz has a broad commercial chancery practice with a particular focus on domestic and international commercial and commercial fraud disputes often involving alleged defaults by trustees or other fiduciaries. Dan has also developed specialist interests in civil contempt proceedings and breach of confidence claims.

Dan is recognised by the main directories as a leading junior in civil fraud, chancery commercial, and company and partnership law; Chambers & Partners 2021 describes him as “A rising star” and “brilliant at what he does”. The directories also emphasise Dan’s excellence in handling clients - “Clients absolutely love him” (Chambers & Partners, 2021); “he is superb with clients, which really marks him out” (Legal 500, 2021) - and his strengths as a team player (“an absolute pleasure to work with” (Chambers & Partners, 2021); “A collaborative team player who is great on detail” (Legal 500, 2021); “Fantastic to lead and work with” (Who’s Who Legal, 2020)). Dan has substantial experience handling trials and heavy applications in both the Chancery Division and the Commercial Court as sole or lead counsel, complemented by a growing arbitration practice. He is also very comfortable as part of a larger counsel team and is currently working with a wide range of leaders, including in matters in the Court of Appeal and the Supreme Court.

Contact Dan McCourt Fritz: clerks@serlecourt.co.uk

ICC FraudNet
Global Annual Report 2022

PART EIGHT

INVESTIGATIONS,
LITIGATION FUNDING
& OTHER
DEVELOPMENTS

Data Science for Investigations: A Practical Guide to Increasing Readiness

Jared Crafton

Current Climate

As we progress through 2022, it is fascinating to reflect on how the world of forensic investigations has evolved through a changing regulatory environment, a global pandemic in its second year, and the rise of the citizen data scientist. On the regulatory front, corruption continues to be a major global issue across industries. One of the biggest trends over the last couple of years is more regulators from other countries getting involved in investigating corruption and levying fines to non-compliant companies. This translates to increased scrutiny on global data, across jurisdictions. Separately, cybersecurity and specifically ransomware attacks continue to outpace counter measures. Law firms and service providers are typically getting several calls a week to respond to incidents. These are example accelerators for an industry that has seen great change in the last two years.

Utilizing data for the purposes of a forensic investigation is now the expectation from regulators, boards, audit committees, and c-suites. The rate of proliferation of data science techniques applied to identify, collect, analyze, and report data has exploded. In an industry that has seen tremendous change over the last ten years, the last two have really shifted the maturity level of forensic data science.

Planning for an Investigation

Companies that have been through the burden of a large, or government, investigation have learned hard lessons about how to organize their data, what data to protect, and what data to they do not need. Relatively small efforts towards information governance can pay big dividends in the ultimate cost of defending an organization from threats inside and out. Organizations that think critically through how they would identify, collect, and analyze their data in the context of an investigation before an event occurs are often surprised at what the current gaps are. Many companies have learned this the hard way through a cybersecurity breach,

and now routinely take steps to streamline response and conduct drills to increase readiness. This methodology is now trickling into the white collar space where more companies are conducting readiness assessments and data house cleaning. Understanding current scientific methods for culling and prioritizing important segments of data allows organization leadership to create “break in case of emergency” response plans that will enable efficient and cost controlled measures without overreaching.

Many organizations conduct enterprise risk assessments on a regular basis, but most do not carry this exercise forward through tactical planning for the data that will be needed should these risks manifest. There are always gaps in data and the institutional knowledge supporting it. Investing a little bit of time in planning for bridging these gaps can save significant time and money should an investigation be necessary.

Investigation Planning

The planning phase is a critical step for the incident response team to think through and memorialize its core mission and the measures that will ultimately determine its success. With the complex environment that global organizations are operating in, a strong data response plan is necessary to corral a diverse group of stakeholders into a shared vision of accountability and action. This is an area that COVID-19 has affected greatly, both in how companies are operating but also in how investigations are being conducted. On the operations side, many companies were unprepared for their workforce to go remote and thus had to quickly implement file sharing and collaboration tools without the luxury of thinking through how this impacts business records. Many companies created new document repositories and had to bypass certain controls which can make it easier to perpetrate fraud and corruption. On the investigation side, just like any other business in this time, companies have had to adapt to conducting more of this work remotely. There are added challenges to not being on-site when conducting an investigation, and like other industries, technology and analytics are called upon to bridge the gap.

Output from the for the planning phase typically includes creation of an overarching incident response plan, drafting success criteria, and establishing relationships that will be called upon in the event of an incident

.

Data Assessment

Before an incident response plan can be implemented, a thorough assessment of the current capabilities, available data, and scope should be developed through a series of interviews, surveys, and testing. While the assessment should be thorough, it does not have to be burdensome. This is typically where organizations are leveraging an enterprise risk assessment ('ERA') as a guide to weigh the risks of business processes, geographies, and operating units. The data assessment phase is about bringing life to the ERA and understanding the nuances of preparing the data that is key to understanding what may have occurred.

A hallmark of thorough data assessments will include metrics defined to assess each individual source of data which is then rated on completeness, accuracy, and usability. A comprehensive data map should be created to show how these pieces fit together into a whole, and a roadmap is created as a tactical plan to piece the data together to answer questions. Example questions such as "Can I get a listing of all donations in our Middle East operation?" can seem simple on the surface, but the complexity of global data means that they rarely are.

The data assessment should have specifics as to how quickly specific information can be obtained, and what should be done with it once acquired. The underlying data of some business platforms can be accessed easily through an Application Programming Interface ('API'), other systems will require custom scripting or even robotic process automation (RPA) for data extraction. RPA is often most helpful in automating the classification, text extraction, and ingestion of unstructured data such as receipts and invoices.

The metrics defined at the beginning of the data assessment will allow an organization to easily understand the benefits and drawbacks of any individual decision regarding what data to collect and how. These decisions can be stored in a data decision log ('DDL'). The DDL safeguards the audit trail and allows the downstream tuning of analytics to account for business rules and data decisions. Creating this in advance can save tremendous time and energy and eliminates the need for trying to document all of this during an investigation.

The output of a Data Assessment can include specific actions to improve current processes, analytics, technology, and record keeping. As part of the assessment, the level of self-sufficiency should be discussed and the reliance on outside parties for assistance a key metric. Should outside vendors be needed for specific tasks such as eDiscovery or forensic accounting, creating a panel of approved vendors and pricing or signing master service agreements in advance can greatly reduce the cost of an investigation.

Incorporating Analytics

Two of the greatest innovations of the last several years has been the rise of the “citizen data scientist” and “no-code” data analysis platforms. This translates to an advancement in the technology and techniques for minimizing the noise that is present in huge corpuses of data, whether that is unstructured data like email or structured data like financial records. An increase in the power and capabilities of analysis tools has allowed investigators to cull huge amounts of information relatively painlessly as opposed to manually reviewing all collected information. What previously took advanced computer science skills can now be accomplished through a series of clicks. This democratization of analytics has brought an influx of ideas and new methods to this space.

Segmentation

With so many geographies, business lines, and policies across global organizations, it is likely that segmentation on the universe of data will need to be performed. Simply put, this is dividing the data into different buckets based on shared attributes. The data segments may differ by something as small as a receipt threshold, or as large as something like country of origin. Each segment will have a different analytics model run against it. This is a common procedure to drive accuracy in detecting exceptions and reducing false positives. Segments are typically identified through a combination of unsupervised machine learning run against the data attributes, translating specific conduct policies into analytics, and institutional knowledge of operations.

Risk Scoring Algorithms

As the analytics program is contemplated, it is critical to map targeted analytics to the specific risks that were identified in the assessment phase as opposed to selecting analytics in a vacuum. Any effective analytics program will consider the various factors that increase coverage for these primary risks. While indicators are themselves not confirmation of impropriety, multiple indicators on a singular entity will show increased risk. An example of this is a payment to a vendor that hits on multiple risk indicators such as round amounts, payments on weekend, and payment on the same day as the invoice. Risk scores can be aggregated at different levels, such as scoring all payments can be rolled up to the vendor level. Risk scoring is typically used early in an investigation to prioritize the reviewer’s time.

Optimization and Artificial Intelligence

Optimizing analytics results is an iterative process. Individual analytics must be tuned to achieve maximum detection accuracy and minimum false positivity. Tuning is performed by iterating through variations of the individual test thresholds, weighting of individual tests within a model, and testing data segments. Accuracy can often be improved by relying on artificial intelligence to detect patterns that are not apparent to the human eye.

Artificial intelligence is utilized within investigations in several different ways. Natural Language Processing ('NLP'), unsupervised machine learning, supervised machine learning, and robotics provide advanced lenses for both identifying potential risks and reducing false positives. For example, NLP can be used for identifying and classifying transaction descriptions which allows for separating the analysis from any potential bias that may be imparted on the data through keyword searching alone. In the early stages of an investigation, a sample of transactions can be reviewed and then supervised machine learning can be run to tune the thresholds and weights of the individual analytics. In a later stage of the investigation, unsupervised machine learning can be used to perform 'below the line' testing on the set of transactions that were not identified as high risk. These techniques can provide comfort that the biggest risks are being identified and mitigated, while maximizing the investigator's available time to focus on the issues that matter most. As previously mentioned, there is a plethora of new software and analysis platforms that can provide these advanced analytics without a huge investment of money or in data science skills.

Reporting

In evaluating a response to an investigation, analytics are only as good as the ability to understand them. A reporting plan does not have to be state of the art - it needs to display the fact pattern and be defensible. Generally, it is worthwhile to explore what kind of reports will make sense of the data being investigated and reports that will show the overall investigation progress. Many organizations have invested in data visualization software that have made this easier, but it may not have made its way to the investigation team.

Interactive dashboards can be utilized to highlight overall program management, risk scoring by vendor, approver, transaction, geographic breakdown, link analysis, trends, and much more. These dashboards allow an investigator to begin their analysis at a global level and quickly drill down into individual business units, vendors, employees, etc.

Review

There are many potential pitfalls around the process of implementing analytics, and one of those is not considering the human factor when designing a testing plan. Running analytics can quickly identify a vast amount of information that needs to be reviewed by investigators. A key consideration to the analytics is the capacity of the team to review the output. An effective review strategy will maximize the investigator's valuable time and drive a comfortable level of accuracy.

Utilizing case management software, allows the efficient review of analytics output and enables more advanced techniques such as supervised machine learning. The data that the investigator reviews is fully tracked, and predictive models can be built based on how the investigator has made decisions. Case management programs typically enable standardized questionnaires, uploading supporting documentation and tagging transactions as something resolved, something to be escalated, or a false positive. Over time, the case management module becomes an important repository of institutional knowledge. This will help create efficiencies when researching new issues, identifying trends, planning for employee turnover, and more. Security within the case management platform allows for different users to have different access and enables an automated review hierarchy. For example, an investigator may want to review 100% of analytics above a certain threshold, and then 20% of escalated transactions to be reviewed a second time for quality control purposes. This can be automated including routing specific alert types to specific reviewers, such as Internal Audit, which can help with building expertise in a certain area.

Sustainability

The final area that a well-reasoned incident response plan contains is sustainability. The response plan is a living and breathing entity that needs periodic attention. Businesses and data change frequently as do outside factors such as analytical tools and common fraud schemes. It is important for this process to be evaluated on a regular interval. The metrics designed at the very beginning of the planning stage will be helpful in showing year over year progress in terms of building bridges across business units, removing obstacles, and reliance on third parties.

Similar to review strategy, the adoption of analytics by humans is a potential hurdle for many organizations to overcome. A comprehensive response plan will include provisions for training, reference materials, and support. Like in anything else, first impressions matter. New technology should engage the end user and entice them to continue working with it with minimal stumbles that will jade the user's opinion.

Finally, the next evolution of investigations and incidence response plans is more information sharing and collaboration among organizations. By sharing information of both internal and external threats, companies will be in a better position to defend against coordinated cyber criminals, rogue employees, and state sponsored threat actors.

About the Author



As the Head of Innovation for BDO's Forensic practice, **Jared Crafton** brings over 19 years of experience advancing the scientific maturity of his client's investigations, compliance programs, and litigation matters. Jared specializes in forensic data science providing clients with effective strategies for tackling complex data environments with easy-to-understand analyses and mitigations.

Jared has a passion for education which he uses to catalyze sustainable solutions that provide a lasting impact. Jared has served as an expert witness in the areas of data mining, data science, and damages. Prior to joining BDO, Jared was a Principal at a Big 4 accounting firm.

Contact Jared Crafton: T. 646 283 9270; E. jcrafton@bdo.com

Resisting Challenges to Funding in Claims Against Fraudsters

Christopher Camponovo and Kirt Gallatin

Abstract

Drumcliffe Partners is a private investment management firm overseeing portfolios of high-value claims pursued on behalf of the victims of fraud, corruption, and abuse of power. Since its founding in 2010, Drumcliffe has financed and managed asset recovery, insolvency, and third-party liability claims in over 30 countries. Increasingly, more brazen defendants are willing to actively resist claims against them, despite the harm that publicizing their wrong doing would bring to their defense, and their reputation. This resistance includes attacks on the funder if fraudsters become aware that such an arrangement exists. These attacks can take a variety of forms, including direct challenges within the claim, collateral attacks in other jurisdictions, and attempts at public messaging. In this article, Chris Camponovo and Kirt Gallatin of Drumcliffe describe some of these tactics, and the considerations to defend against them.

Claim-Related Challenges

Not surprisingly, defendants accused of fraud often have the financial resources to actively resist asset recovery claims by using the very fruits of their wrongdoing to pay for their defense. Indeed, they rely on any line of attack available, including against the funder. These can include challenges based on historic legal strictures on the practice of funding, abuse of the discovery process to make funding arrangements public, and attempts to drive up the costs of litigation to dissuade a funder from continuing to finance the claim.

Champerty and Maintenance

While all ICC FraudNet member law firms are well versed in the laws limiting, or even prohibiting, third-party funding of lawsuits, it is important to consider the current state of these somewhat archaic laws with respect to funders. This is

because in many of the jurisdictions fraudsters use to conceal their assets, these laws have not been entirely broken down or eliminated.

Historically, third-party funding of litigation was prohibited by the common law crimes of champerty and maintenance, *i.e.*, a claimant could not agree to provide a third-party a part of any award in exchange for funding the claims. Although these “crimes” have largely been expressly abolished or rendered irrelevant in most jurisdictions, including, *e.g.*, in the U.K., the U.S. and Australia, some ambiguity remains. Indeed, it was only last year in a case funded by Drumcliffe, that a court in the British Virgin Islands published an opinion squarely addressing the issue. In *Russell Crumpler et al v Exential Investments Inc (In Liquidation)*, the court approved the use of a litigation funder by liquidators in an insolvency. While litigation funding was common in the BVI before *Exential*, the decision was the first written ruling that expressly approved the practice. Judge Adrian Jack wrote:

In my judgment, the funding arrangement proposed is not contrary to BVI public policy. Indeed, the contrary is the case. Without the funding, the liquidators would be unable to obtain recoveries for the benefit of the creditors of the company. Approving the funding arrangement is in the current case essential to ensure access to justice.¹

Other offshore jurisdictions have similarly approved third-party funding agreements, including in the Cayman Islands, Bermuda, and Jersey. However, it is noteworthy that there are a number of holdouts (*e.g.*, Ireland) and many jurisdictions allow third-party funding in limited circumstances (*e.g.*, Hong Kong). As a result, the permissibility of litigation funding is governed by an inconsistent patchwork of legislation and case law, inconsistency which may be available to a defendant seeking to invalidate funding used by a victim of fraud to recover stolen assets.

For instance, in some jurisdictions the courts have expressly permitted third-party funding in insolvency cases, but it remains an open question as to whether it would be similarly permitted in other claims, such as asset recovery claims against fraudsters. While there is a strong case that claims by victims of fraud would not otherwise be brought, but for litigation funding, and as such it qualifies as public interest litigation, this is a potential vulnerability that a well-resourced defendant may attempt to exploit. Indeed, where there continue to exist holdouts where the application of the doctrines of champerty and maintenance is at least ambiguous, it will be raised by defendants if and when they learn a case is financed by a third-party funder.

¹ *Russell Crumpler et al v Exential Investments Inc (In Liquidation)*, Claim No. BVIHC (COM) 81 of 2020.

Discovery-related Attacks

In the mid-2000's, Mohammad Al-Saleh collaborated with International Oil Trading Company, LLC ('IOTC') in procuring and executing contracts to transport fuel on behalf of the United States military. The relationship eventually soured, and Mr. Al-Saleh sued IOTC. Mr. Al-Saleh entered into a funding agreement with Burford Capital to fund his litigation. He was victorious against IOTC and, after years of trying to collect on the judgment, filed an involuntary bankruptcy petition against IOTC. IOTC responded, in part, by arguing that Mr. Al-Saleh had transferred an interest in the judgment debt to its litigation funder, Burford Capital, and his role as petitioning creditor was therefore inappropriate. IOTC subsequently filed a request for production of all documents between Mr. Al-Saleh and Burford including funding agreements and all written communications. Mr. Saleh objected and claimed that all the responsive documents were subject to attorney-client privilege, common interest/joint defense privilege, and work product protection - raising an "...outstanding and novel question of law..."²

The court ruled that while Burford was not Mr. Al-Saleh's attorney, their communications were nevertheless protected by both the common interest exception and the agency exception. Adopting the more expansive "common enterprise" approach to the common interest exception, the court found that the communications were necessary to "obtain informed legal advice, specifically advice as to how to prosecute a collection action against IOTC USA and how to fund that action."³

The court also ruled that, under federal and Florida state law, the communications were protected under the agency exception: "...these provisions are intended to protect communications with any party who assists the client in obtaining legal services. Litigation funders fall in this category."⁴

The court could have finished its analysis there but continued and deemed that the Burford communications were also considered "work product" and therefore protected under Fed. R.Civ.P. 26(b)(3). As the court reasoned, the communications between Mr. Al-Saleh, his attorney, and his litigation funder were opinion work product with "the primary motivating purpose...to aid in possible future litigation."⁵

After its analysis, the court denied the vast majority of IOTC's motion to compel. It only required Mr. Al-Saleh to produce his funding agreement with Burford - after

² *In re International Oil Trading Co.*, 548 B.R. 825, 831 (Bankr. S.D. Fla. 2016).

³ *Id* at 833.

⁴ *Id* at 834.

⁵ *Id* at 837 citing *U.S. v. Davis*, 636 F.2d 1028, 1040 (5th Cir.1981).

redacting any terms of payment and any terms he reasonably believed may disclose mental impressions and opinion in relation to his litigation with IOTC.⁶

A claimant sometimes needs assistance from a reputable litigation funder. Unfortunately, fraudsters will try to exploit the manner in which a claim is funded to avoid accountability, much like IOTC attempted to in this case with its discovery requests. While the issues presented here have now been resolved in US courts, there are still some unresolved issues in other jurisdictions that defendants may use against claimants partnering with litigation funders.

Security for Costs

One common tactic to frustrate a victim's attempts to recover assets is to drive up the cost of litigation in order to deter the funder from continuing to finance the claim. In cost-shifting jurisdictions, the losing party will pay a substantial proportion of the winning party's legal costs. Where a defendant wishes to drive up costs, he will argue that the claimant is unable or unwilling to pay any costs awarded against it and request that the claimant provide security for the costs it may become liable to pay. The order will usually require the claimant to pay money into court or provide some other security before it is allowed to proceed with the claim. Fraudsters, knowing they are the target of a valid claim, will exploit this procedure to delay litigation and make the litigation financially unfeasible for the claimant and its funders.

Security for costs can also be pursued against an entity outside the jurisdiction if there is reason to believe the claimant will be unable to pay any adverse costs award made against it. Evidence will be presented to the court to show:

- that the claimant's finances are, or potentially are, in an uncertain state; and
- the amount of costs, actual and future, that the claimant may be liable to pay.

If the court is persuaded by the defendant's application, then it has the discretion to order that security be given. Notably, if security for costs would prevent a claim from being filed (*e.g.*, in the case of public interest litigation), a court will not require it. However, if a case is funded, this is a difficult argument for a claimant to win because it is assumed that a funder is capable of posting security.

⁶ *Id* at 839.

One of the primary reasons a claimant may seek funding is that they are financially incapable of pursuing their claim themselves, making them easy targets for canny defendants to apply for an order for security for costs. Under CPR 24.15⁷, the burden may then be saddled on the third-party funder - whether by tying up its own capital or acquiring after the event ('ATE') insurance - potentially discouraging them from investing in the claim, placing the claimant at a disadvantage, and potentially preventing the claim or appeal from proceeding further.

Indemnity Principle

In English common law, the indemnity principle basically means that a successful party cannot recover more in legal costs than they are liable to pay their solicitor. But what if a solicitor's legal costs are being provided by a third-party funder, and the claimant has no liability to pay those costs? Should a defendant be able to avoid paying the claimant's legal costs if the claimant does not have to pay them?

Defendants will attempt to argue that they should not have to pay costs - essentially to the funder - if the claimant is not paying its own legal costs. English courts have, to the benefit of claimants, been unpersuaded by such arguments. In *HMRC v. Gariner and others*, the claimants were taxpayers challenging penalties imposed by Her Majesty's Revenue and Customs ('HMRC'). The taxpayers were triumphant, and HMRC was ordered to pay the claimants' legal costs. However, the legal fees were paid by claimants' tax advisors - EDF Tax Defence Ltd ('EDF'). HMRC argued that the order requiring it to pay legal costs violated the indemnity principle.

The court rejected HMRC's arguments, writing: "It is liability to pay rather than who makes payment which is material."⁸ While the claimants in this case were not personally paying their legal costs, the legal costs had to be paid. HMRC, as the losing party, was therefore liable for costs. Conversely, a third-party funder can be liable for a defendant's cost if the claimant is unsuccessful.

In *Excalibur Ventures LLC v Texas Keystone Inc & Ors*, the court found that litigation funders are liable to pay indemnity costs awarded against the claimant. The court reasoned that a litigation funder cannot dissociate itself from its client. Litigation funders "follow the fortunes of those from whom [they] hoped to derive a small

⁷ "The defendant may seek an order against someone other than the claimant, and the court may make an order for security for costs against that person if it is satisfied...that it is just to make such an order and...the person has contributed or agreed to contribute to the claimant's costs in return for a share of any money or property which the claimant may recover in the proceedings..."

⁸ *HMRC -v- Gardiner and Others* [2018] EWHC 1716 (QB).

fortune” and that meant being held jointly liable for the indemnity costs ordered against the claimant.⁹

In the past, funders had the benefit of the “*Arkin* cap”, but that has lost favor in the courts. In *Arkin v Borchard*, a claimant brought proceedings that cost £1.3 million in third-party funding. The claim failed, and the defendants sought to recover costs of almost £6 million from the funder. The court held that the funder should be liable for costs, but only up to the amount of funding provided. This became known as the “*Arkin* Cap.”¹⁰ This was a well-received opinion as it limited the risk for any third-party funder.

However, further guidance on the *Arkin* cap was given in *Excalibur*. The court stated the *Arkin* cap should include both the amount a funder provided for the claimant’s costs and the amount provided for security for costs. Consequently, payment of security for costs is simply part of the costs required to be met to be able to pursue the claim.¹¹

Finally, in *Davey v Money & Others* the court found that the *Arkin* cap was not a bright line rule to be applied automatically, but “an approach which...should be considered for application in cases involving a commercial funder as a means of achieving a just result in all the circumstances of the particular case.”¹²

Ultimately, the court has broad discretion to what extent a funder should be liable for adverse costs. For funded cases, this means a defendant will attempt to drive up the funder’s costs in pursuing the litigation, but there are no bright line rules. If the case is on behalf of a victim of fraud or corruption, the equities may lie with the claimant and the funder and, therefore, weigh against a defendant’s attempts to stack the litigation deck against the claimant. If, however, it is simply a commercial litigation, a defendant’s attempts to drive up costs for the funder may get more traction.

Collateral Attacks in Other Jurisdictions

U.S. federal law provides a tool for parties engaged in, or about to engage in, litigation in a foreign forum: 28 U.S.C. § 1782. The statute allows a litigant to request that a court issue discovery subpoenas in the United States for use in a foreign proceeding. A federal court will issue a subpoena if the applicant: (a) has an interest in the foreign proceeding; (b) the discovery will be used in that foreign proceeding;

⁹ *Excalibur Ventures LLC v Texas Keystone Inc & Ors* [2016] EWCA Civ 1144

¹⁰ *Arkin v Borchard Lines Ltd* [2005] EWCA Civ 655 [2005] 1 WLR 3055.

¹¹ *Excalibur Ventures LLC v Texas Keystone Inc & Ors* [2016] EWCA Civ 1144

¹² *Davey v Money and others* [2019] EWHC 997 (Ch)

and (c) the target of the discovery request resides in the judicial district where the request is made.¹³

1782 is an important tool used by plaintiffs in asset recovery claims, but given the low hurdle a litigant needs to meet under section 1782, this provision is also used by defendants - at times to attack funders, in particular by seeking to obtain, for example, funding agreements and other confidential investor information.¹⁴ The applicant does not need to be a litigant in the foreign proceeding and can be anyone who “merely possess[es] a reasonable interest in obtaining the assistance.”¹⁵ The foreign proceeding is not limited to litigation in front of a foreign court but may also include quasi-judicial proceedings such as investigating magistrates or administrative and arbitral tribunals.¹⁶ Finally, the foreign proceeding does not need to be ongoing, or even imminent. The only requirement is that the evidence sought will eventually be used in a proceeding sometime in the future.¹⁷ This gives US federal courts broad discretion to grant section 1782 applications.

The goal of this discovery on behalf of defendants is two-fold. First, if deep-pocketed defendants can obtain sensitive material that isn't considered privileged (because it is in the possession of a third party), they can obtain an unfair look into the overall recovery strategy of the plaintiff and potentially move assets to other jurisdictions pre-emptively, before they can be frozen. Second, the very act of obtaining discovery is often time-consuming and onerous. If defendants can drive up costs for a funder, or create a nuisance for them that is collateral to their investment (*i.e.*, their asset recovery strategy), the intent is to dissuade them from providing additional capital to the client going forward.

Notably, section 1782(a) expressly shields privileged material, which extends a level of protection to funders when they can show their communications and other materials benefit from a privilege.¹⁸ Of course, the costs of defending against attempts to probe confidential, sensitive materials are not insignificant. This provides wrongdoers with another line of attack against a funder supporting litigation in a jurisdiction outside the United States.

Public Messaging

¹³ *Intel Corp. v. Advanced Micro Devices, Inc.*, 542 U.S. 241, 264-65 (2004).

¹⁴ *In re Ex Parte Application of Eni S.p.A. for an Order Pursuant to 28 U.S.C. section 1782 Granting Leave to Obtain Discovery for Use in Foreign Proceedings* (Case No. 1:20-mc-00334-MN).

¹⁵ *Intel Corp at 264-65* (2004) *citing* Smit, *International Litigation under the United States Code*, 65 Colum. L. Rev. 1015, 1027 (1965).

¹⁶ *Id.*

¹⁷ *Id.*

¹⁸ “A person may not be compelled to give his testimony or statement or to produce a document or other thing in violation of any legally applicable privilege.”

Litigation funders may also be targets if a wrongdoer attempts to control the public narrative by shifting attention away from itself and, at the same time, vilifying the funder. This includes the use of leaks to the media, press releases, and websites.¹⁹ This is particularly true with high-profile claims - and the larger the quantum, the more money the wrongdoer is willing to spend to defame the funder (and defeat the claim).

Given the general lack of information about what litigation funders do, in particular, how they can enable claims to recover assets by the victims of fraud, corruption, and abuse of power, they are particularly susceptible to attempts to color them as opportunistic, rapacious private equity marauders. While it is difficult to draw a direct line between a media narrative and a judge's opinion; judges and their clerks read newspapers and may sometimes formulate opinions on the policy merits of a matter without first reviewing the legal merits. For this reason, defendants with resources to spare will do what they can to discredit funders in the court of public opinion. For our own part, Drumcliffe will not finance an asset recovery claim where we stand to profit more than the actual victim of the fraud, both as a matter of principle, and practicality. Courts must know that our role in a claim is to assist impecunious victims, not to take advantage of them.

Lessons Learned

As detailed above, fraudsters and the parties who assist them have at their disposal a number of tools to frustrate attempts to recover assets for victims. However, there are several precautionary measures a litigation funder can take to mitigate the negative impact of these challenges.

First, litigation funders should consider the tactical advantages and disadvantages of making a funding relationship public or maintaining confidentiality. This is a fact-dependent analysis, and the result will be different depending on the situation, the jurisdiction, and the parties. In some cases, full transparency is advisable, particularly where further publicizing the wrongdoing advances the claims before the court. In others, the funder may choose to keep its funding arrangement confidential for as long as possible, especially against deep-pocketed third parties in jurisdictions where the tactics highlighted above may gain traction. What is important is that a funder recognize that each option has its pros and cons, and that

¹⁹ In connection with litigation over the OPL 245 fraud in Nigeria, Eni put this tactic to use on a webpage it created specifically related to the criminal charges and civil claims made against the company and its employees in various jurisdictions. See, e.g., <https://www.eni.com/en-IT/media/opl245-case-process-nigeria/case-shell-eni-delaware.html> (last visited Dec. 21, 2021).

a conscious decision is taken early enough in the proceedings to adopt measures to protect the position.

Second, litigation funders need to ensure maximum coverage of privilege (*i.e.*, attorney client communication, work product, common interest). All letters of engagement, funding agreements, terms sheets, etc. should reflect common interest and applicability of privilege. This will serve to protect work product from attempts by wrongdoers to utilize the discovery process to frustrate a funder.

Third, funders must be careful not to control the litigation or otherwise direct strategy. While some jurisdictions allow the funder to sit in the driver's seat, the majority do not. Defendants may try to prove that a third-party funder is pulling the strings from behind the scenes. For this reason, it is critical that a claimant engage counsel with the knowledge and experience that provides a funder with confidence in the asset recovery strategy being implemented.

Finally, a funder must budget for the worst-case scenario. In cost-shifting jurisdictions, this means considering both their estimated costs and the costs of putting up security for costs. In other words, a funder may not be able to self-insure against costs awards and pay an amount equivalent to the defendant's estimated costs into court or obtain ATE insurance, which can cost upwards of 50% of the defendant's estimated costs.

Over the past fifteen years, asset recovery finance has evolved to become an important tool to assist the victims of fraud and corruption in obtaining restitution. Unfortunately, techniques to frustrate these efforts have also evolved. As a consequence, asset recovery finance has become more expensive, but with careful planning, funders, lawyers, and victims can stay one step ahead of their unscrupulous adversaries.

About the Authors



Christopher N. Camponovo is Managing Director at Drumcliffe Partners. Chris has over 20 years of experience working in government and the private sector. He has held senior positions at the White House and U.S. State Department. Chris has spoken, written and published articles on a diverse range of topics, including U.S. foreign investment treaties, international human rights, and corporate ethics. He holds a JD from the University of California Los Angeles Law School, and a BA from UC San Diego.

Contact Christopher Componovo and Kirt Gallatin at: info@drumcliffepartners.com

Kirt W. Gallatin is a Director at Drumcliffe Partners. His professional background focuses government, elections, and law. Prior to joining Drumcliffe, he serving as the Director of Policy for the U.S. Department of Commerce's International Trade Administration. He has advised several Heads of State on pre- and post-election strategy, and practiced law, specializing in civil litigation. He holds a JD from Northwestern University Pritzker School of Law, and a BS from Florida Gulf Coast University.



Searching for the debtors' bank accounts across European Union: the EAPO Regulation information mechanism

Carlos Santaló Goris

Abstract

In this article, Carlos Santaló Goris, a Research Fellow at the Max Planck Institute for International, European and Regulatory Procedural Law, provides a general overview of the mechanism set forth in the European Account Preservation Order Regulation (Regulation No 655/2014) to gather information about debtors' bank accounts. Carlos puts a special focus on the functioning of this instrument, relying on empirical qualitative data gathered from German, Spanish and Luxembourgish practitioners, courts, and authorities with first-hand experience in this area.

Introduction

On 17 January 2017, Regulation No 655/2014 establishing a European Account Preservation Order ('EAPO') entered into force,¹ bringing to life the very first European civil provisional measure. The EAPO Regulation is one of three specific instruments resulting from the European Commission's efforts to improve the recovery of pecuniary claims within the Area of Freedom Security and Justice. The other two are the European Payment Order;² and the European Small Claims Procedure.³ The EAPO proceeding, as its very name indicates, consists of the temporary attachment of a debtor's bank accounts. It applies in all EU Member

¹ Regulation (EU) No 655/2014 of the European Parliament and of the Council of 15 May 2014 establishing a European Account Preservation Order procedure to facilitate cross-border debt recovery in civil and commercial matters OJ L 189, 27.6.2014, p. 59-92 ("EAPO Regulation").

² Regulation (EC) No 1896/2006 of the European Parliament and of the Council of 12 December 2006 creating a European order for payment procedure, OJ L 399, 30.12.2006, p. 1-32.

³ Regulation (EC) No 861/2007 of the European Parliament and of the Council of 11 July 2007 establishing a European Small Claims Procedure, OJ L 199, 31.7.2007, p. 1-22.

States, except Denmark,⁴ and its scope of application is limited to cross-border civil and commercial claims.⁵

Besides allowing the provisional attachment of bank accounts, the EAPO Regulation also contains a specific proceeding to search them. When a claimant submits an EAPO application, they are allowed to identify the debtor's bank accounts to be attached. In this regard, the EAPO Regulation is rather flexible. Claimants can identify the targeted account through the IBAN; the BIC; or the name and address of the bank which holds the debtor's accounts.⁶ However, creditors are often not privy to such information. Whereas some Member States may have domestic mechanisms to find the debtor's assets, these vary substantially from one Member State to another.⁷ Furthermore, foreign creditors might not be aware of their existence. Further, relying on private investigation agencies could be expensive.⁸ Aware of the potential disruption that such barriers might have on the functioning of the EAPO Regulation, the European Commission decided to include in it an autonomous mechanism to search for debtors' bank accounts.⁹ This mechanism is contained in Article 14 of the EAPO Regulation. This provision combines a set of uniform rules, minimum standards, and numerous references to Member States' national laws. Therefore, the manner in which it is applied varies from one Member State to another. This paper aims at offering an inside view on how the information mechanism is applied at the domestic level, focusing on three Member States: Germany, Luxembourg and Spain.

1. Territorial scope of application

The information mechanism has the same territorial scope of application as the EAPO Regulation. It applies in all Member States, except Denmark as already mentioned, and it is limited to cross-border claims. The creditor's domicile, the bank account to be attached, and the court that renders the EAPO must all be found in a Member State where the EAPO applies.¹⁰ The cross-border element is established through the

⁴ Recital 48 EAPO Regulation.

⁵ On the cross-border element: Article 3 EAPO Regulation. The notion of "civil and commercial" has to be interpreted autonomously, observing what the Court of Justice of the European Union ("CJEU") stated concerning the same equivalent notion in the Brussels I *bis* Regulation (Regulation No 1215/2012): Katharina Hilbig-Lugani, "Artikle 2 EuKoPfvO" in Wolfgang Krüger and Thomas Rauscher (eds.), *Münchener Kommentar zur Zivilprozessordnung, Band 3* (C.H. Beck 2017), margin no. 2.

⁶ Art. 8(1)(c) EAPO Regulation.

⁷ Green Paper - Effective enforcement of judgments in the European Union: the transparency of debtors' assets, COM/2008/0128 final, p. 3.

⁸ Commission Staff Working Paper Executive summary of the Impact Assessment, SEC/2011/0938 final, pp. 16-17.

⁹ *Ibid.* p. 47.

¹⁰ Thomas Rauscher and Denise Wiedemann, "Art 3 EU-KpfvO" in Thomas Rauscher (ed.), *EuZPR-EuIPR: Europäisches Zivilprozess- und Kollisionsrecht* (4th edn, Otto Schmidt 2015), para. 4.

interplay of these three elements. In order to consider that a claim has a cross-border dimension, the debtor's bank account has to be located in a different Member State from the one of the court that grants the EAPO or, alternatively, the one of the creditor's domicile.¹¹ When the bank account information is not known by the creditor, the Member State of the bank accounts would be the Member State where the bank accounts are assumed to be held.

2. The procedure to request and obtain information about the bank accounts

1. Moment of the request for information and competent court

The request for information about the debtor's bank accounts has to be made within the application for an EAPO.¹² The request is submitted through the same pre-established standard form used for the EAPO application.¹³ This standard form contains a specific section dedicated to the information mechanism. Creditors can apply for information about bank accounts in more than one Member State. Even if creditors have already included the details of some bank accounts in the EAPO application, they are not prevented from requesting information about other bank accounts that the debtor might have.¹⁴ The court that examines that application for the information is the same that decides on the application for the EAPO.

The information obtained about the debtor's bank accounts serves exclusively to complete the EAPO application. This means that claimants cannot use the EAPO Regulation solely to collect information about the debtor's bank accounts;¹⁵ and that the information obtained through the information mechanism cannot be used for purposes outside the EAPO proceeding.¹⁶

¹¹ Art. 3 EAPO Regulation.

¹² Art. 8(1)(v). In this sense: Nils Harbeck, "Art. 14 EuKoPfVO" in Johann Kindl, and Caroline Meller-Hannich, *Gesamtes Recht der Zwangsvollstreckung* (Nomos 2021), para. 1.

¹³ All the mandatory standard forms of the EAPO proceeding are contained in the EAPO Commission Implementing Regulation. They can be filled-in only through the e-Justice portal. It presents one major advantage: once the form has been completed, it can be translated automatically into any other EU official language, except Gaelic. See: https://e-justice.europa.eu/378/EN/european_account_preservation_order_forms?clang=en (accessed on 15 November 2021).

¹⁴ Hubertus Schumacher, "Art 14" in Hubertus Schumacher, Barbara Köllensperger and Martin Trenker (co-authors), *EuKoPfVO: Kommentar zur EU-Kontenpfändungsverordnung* (Manz 2017), margin no 8.

¹⁵ Hilbig-Lugani (n 5), para. 2; Matthias Klöpfer, 'Art 14 Verordnung (EU) Nr 655/2014' in Reinhold Geimer and Rolf A Schütze (eds), *Internationaler Rechtsverkehr in Zivil- und Handelssachen* (CH Beck 2016) margin no 2.

¹⁶ Contra: Burkhard Hess, "Art 14 EuKtPVO" in Peter F Schlosser and Burkhard Hess (eds), *EU-Zivilprozessrecht: EuZPR* (4th edn, CH Beck 2015), para 2.

II. Prerequisites to access the information mechanism

a. Only creditors with a title

Claimants can apply for an EAPO *ante demandam*; during the proceeding on the merits of the claim; or when the creditor has already obtained a title.¹⁷ Nonetheless, the information mechanism is limited to those creditors who have obtained a title.¹⁸ In fact, while the Commission's EAPO Proposal was more flexible, making the information mechanism available for all creditors,¹⁹ upon review by the Council it was decided to restrict the recourse to such mechanism to creditors with a title, only.²⁰ However, the title does not have to be enforceable.²¹

b. General prerequisites to obtain an EAPO

Before accepting the creditor's request for information, courts have to verify that all the general prerequisites to obtain an EAPO are duly satisfied.²² For obvious reasons, the only exception is the information about bank accounts. Creditors must prove that there "is a real risk that, without such a measure, the subsequent enforcement of the creditor's claim against the debtor will be impeded or made substantially more difficult".²³ Besides the so-called *periculum in mora*, a creditor with a non-enforceable title "shall also submit sufficient evidence to satisfy the court that he is likely to succeed on the substance of his claim against the debtor".²⁴ Unless exempted by the court, creditors also have to provide a security.²⁵ In

¹⁷ Art. 5 EAPO Regulation.

¹⁸ Art. 14(1)(2) EAPO Regulation.

¹⁹ Art. 17 COM/2010/0748 final.

²⁰ France was the most explicit supporter of a more restrictive access regime, asking to restrain the information mechanism just for the use of those creditors who had obtained enforceable title (Comments on Chapters I, II and III from the French delegation, 13260/11 JUSTCIV 205 CODEC 1280, 13140/12 ADD 13,) On the legislative discussions about which creditors should have access to the information mechanism: Georgios Orfanidis, 'Die Verordnung (EU) Nr. 655/2014 des Europäischen Parlaments und des Rates über ein europäisches Verfahren zur vorläufigen' in Klaus J. Hopt und Dimitris Tzouganatos (eds.), *Das Europäische Wirtschaftsrecht vor neuen Herausforderungen. Beiträge aus Deutschland und Griechenland* (Mohr Siebeck 2014), p. 263.

²¹ Art. 14(2) EAPO Regulation.

²² Franz Mohr, *Europäischer Beschluss zur vorläufigen Kontenpfändung: EuKoPfVO* (LexisNexis 2014), margin no. 204.

²³ Art. 7(1) EAPO Regulation. Defending a more lenient application of this prerequisite for those creditors with an enforceable title, see: Burkhard Hess, "Towards a more coherent EU framework for the cross-border enforcement of civil" in Jan von Hein and Thalia Kruger (eds.), *Informed Choices in Cross-Border Enforcement. The European State of the Art and Future Perspectives* (Intersentia 2021), p. 395.

²⁴ Art. 7(2). The text of the EAPO Regulation indicates that this prerequisite affects only those creditors without a title, without any reference to the enforceability of the title. However, the CJEU has clarified that creditors with a non-enforceable title have the same status as creditors concerning the prerequisites to obtain an EAPO: C-555/18, 7 November 2019, *K.H.K. (Account Preservation)*, ECLI:EU:C:2019:937, para. 42.

²⁵ Art. 12 EAPO Regulation.

principle, the amount of that security is calculated based on the potential damages that the EAPO might cause to the claimants.²⁶

c. Reasons to assume that debtor has bank accounts in a Member State

The creditor cannot request the investigation of the debtor's bank accounts in whichever Member State they might like to. They have to show a connection between the debtor and the Member State where the bank accounts may exist.²⁷ This prerequisite, which did not appear in the Commission's EAPO Proposal,²⁸ was introduced to prevent creditors from using the information mechanism for fishing expeditions.²⁹ The link between the debtor and the Member State could be established, for instance, if the debtor has assets or exercises a professional activity in the Member State.³⁰

d. Additional prerequisites for creditors with a non-enforceable title

When the title is not yet enforceable, creditors need to satisfy three additional prerequisites.³¹ The purpose of this stricter access regime is to compensate, precisely, for the lack of enforceability of the title.³² According to the first prerequisite, "the amount to be preserved has to be substantial". This has to be determined in light of the circumstances of the claim.³³ Secondly, there has to be "an urgent need for account information because there is a risk that, without such information, the subsequent enforcement of the creditor's claim against the debtor is likely to be jeopardised". This prerequisite sounds very much like the general *periculum in mora* that all creditors have to satisfy to obtain an EAPO. Still, they should not be combined and have to be justified separately.³⁴ Finally, not obtaining the information about the bank accounts has to cause "substantial deterioration of the creditor's financial situation".

²⁶ Alternatively, "in the absence of specific evidence as to the amount of the potential damage", they could rely on the amount of the claim as a term of reference to calculate the amount of the security: Recital EAPO Regulation.

²⁷ Art. 14(1) EAPO Regulation.

²⁸ Art. 17(1) COM/2011/0445 final.

²⁹ Hess (n 14), para 2.

³⁰ Recital 20 EAPO Regulation.

³¹ Art. 14(1) EAPO Regulation.

³² Harbeck (n 12), para 12.

³³ Some scholars suggest that there is a minimum threshold of 1,000 euros and no amount below that would be considered substantial: Manfred Mann-Kommenda, "Artikle 14 EuKoPfVO" in Andreas Geroldinger and Matthias Neumayr (eds.), *IZVR. Praxiskommentar Internationales Zivilverfahrensrecht* (LexisNexis 2021), margin no. 9.

³⁴ Gilles Cuniberti and Sara Migliorini, *The European Account Preservation Order Regulation: A Commentary* (Cambridge 2018), p. 178. In practice it is very likely that courts might interpret them in the same manner: Hubertus Schumacher, "Art 14" in Hubertus Schumacher, Barbara Köllensperger and Martin Trenker (co-authors), *EuKoPfVO: Kommentar zur EU-Kontenpfändungsverordnung* (Manz 2017), margin no 51.

III. *Sending the request for information*

Once the court has verified that all the prerequisites to access the information mechanism are duly satisfied, it will send the request to the information authority in the Member State where the bank accounts are assumed to exist.

IV. *Retrieving information about the bank accounts*

Information authorities are the bodies in charge of searching for the debtor's bank accounts.³⁵ Each Member State had to select a national information authority by 18 July 2016.³⁶ The EAPO Regulation gave Member States freedom to pick whichever domestic body they consider more suitable to become an information authority.³⁷

Article 14 provides three examples of methods that could be used by information authorities to search for the debtor's bank accounts.³⁸ The first method consists of asking all the banks in the Member State of the information authority to disclose if they have the accounts of the debtor.³⁹ According to the second method, information authorities could gather the information from national registries held by other public authorities.⁴⁰ Finally, courts could also ask debtors to disclose if they have bank accounts in the Member State of the information authority.⁴¹ Since the EAPO is granted *inaudita altera parte*,⁴² in order to preserve its surprise effect, the request to the debtor has to be "accompanied by an *in personam* order by the court prohibiting the withdrawal or transfer by him of funds held in his account or accounts up to the amount to be preserved by the Preservation Order".⁴³ This list of methods is not *numerus clausus*, and Member States can opt for a different one as long as it

³⁵ All information about the information authorities can be found in the European Judicial Atlas: https://e-justice.europa.eu/content_european_account_preservation_order-379-en.do (accessed on 15 November 2021).

³⁶ Art. 50(1)(b) EAPO Regulation.

³⁷ Nonetheless, some domestic bodies might be more suitable than others. The Cyprian government consulted the European Central Bank about the appointment of the Cyprian Central Bank as the information authority. While the ECB did not expressly stand against such appointment, it considered the information authorities' tasks "are atypical for a central bank" and recommended "that further consideration should be given the designation of the CBC as the information authority for the purposes of the Regulation" (ECB, *Opinion of the European Central Bank of 21 August 2017 on the designation of the Central Bank of Cyprus as the information authority and inclusion of relevant exception to bank secrecy requirement* (CON/2017/32), p. 6.

³⁸ Art. 14(5) EAPO Regulation.

³⁹ Art. 14(5)(a) EAPO Regulation

⁴⁰ Harbeck (n 12), para. 12.

⁴¹ Art. 14(5)(c) EAPO Regulation.

⁴² Art. 11 EAPO Regulation.

⁴³ This method did not appear in the Commission's EAPO Proposal (Art. 17(5) COM/2011/0445 final). It was introduced upon the request of the United Kingdom (Comments on Chapters I, II and III from the delegation of the United Kingdom, 13140/12 LIMITE, 13260/11 JUSTCIV 205 CODEC 1280, p. 11). Austria and Malta are the only two Member States which have relied on this system: < https://e-justice.europa.eu/content_european_account_preservation_order-379-en.do > (accessed on 15 November 2021).

is “effective and efficient for the purposes of obtaining the relevant information” and “not disproportionately costly or time-consuming”.⁴⁴

Information authorities cannot transmit any kind of information about the debtor’s bank accounts they might like to. They are bound by the principle of data minimization enshrined in Article 47 of the EAPO Regulation.⁴⁵ In the context of the information mechanism, this means that the information transmitted shall be limited to that strictly necessary to identify the bank accounts, which could be the IBAN; the BIC; or the name and address of the banks.⁴⁶ Anything beyond that information (e.g. account balances, transfers made by the creditor), would be contrary to the referred principle of data minimization.

There is no specific deadline to reply to the court’s request for the information. Article 14 merely states that “all authorities involved in obtaining the information shall act expeditiously”.⁴⁷ Information authorities always have to give an answer to the requesting court, even if they do not find any bank accounts.⁴⁸

V. *The decision on the EAPO application*

Once the court receives the answer from the information authority, it renders the decision on the application for the EAPO.⁴⁹ If no bank accounts were found, and the creditor does not have the details of any other bank account, then the court will not issue the EAPO.⁵⁰

3. The information mechanism in the practice

I. *Reliance on the information mechanism*

Available statistics about the EAPO Regulation in Germany, Luxembourg, and Spain reveal that it has been scarcely used.⁵¹ In 2020, in Germany, there were just 34

⁴⁴ Art. 14(5)(d) EAPO Regulation.

⁴⁵ Art. 47(3) EAPO Regulation: “personal data which are obtained, processed or transmitted under this Regulation shall be adequate, relevant and not excessive in relation to the purpose for which they were obtained, processed or transmitted”. This article reproduces Article 5(1)(c) of the General Data Protection Regulation: “personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed”.

⁴⁶ Art. 8(2)(d) EAPO Regulation.

⁴⁷ Cuniberti and Migliorini consider that, ideally, information authorities should provide an answer to the requesting court within the next three or four working days upon reception of the information request: Cuniberti and Migliorini (n 34), p. 181.

⁴⁸ Thomas Rauscher and Denise Wiedemann, “Art 14 EU-KpFVO“ in Thomas Rauscher (ed.), *EuZPR-EuIPR: Europäisches Zivilprozess- und Kollisionsrecht* (4th edn, Otto Schmidt 2015), margin no 19.

⁴⁹ Franz Mohr, *Europäischer Beschluss zur vorläufigen Kontenpfändung: EuKoPfVO* (LexisNexis 2014), margin no 224.

⁵⁰ Carl Friedrich Nordmeier and Julia Schichmann, “Der Europäische Beschluss zur vorläufigen Kontenpfändung“, *Recht der Internationalen Wirtschaft* (2017), p. 410.

⁵¹ Following Article 53 of the EAPO Regulation, Member States have to data about “the number of applications for a Preservation Order and the number of cases in which the Order was issued”.

EAPO proceedings.⁵² In that year, in Luxembourg, there were just 19 EAPO applications;⁵³ while Spanish courts just issued 23 EAPOs.⁵⁴ Nonetheless, a significant number of those applications might have included information requests. Many of the EAPO applications identified through interviews conducted with lawyers, judges, and court officers in those Member States contained information requests.⁵⁵ In Luxembourg, information requests represented up to 78% of the EAPO applications.⁵⁶ In Spain and Germany, creditors asked to investigate the debtor's bank accounts in around 69% and 44% of the EAPO applications, respectively.⁵⁷ Taking into consideration the limited number of EAPO requests, use of the information mechanism was relatively widespread. It appears that obtaining information about debtors' bank accounts is also one of the main reasons among the lawyers of these Member States for submitting an EAPO application. This strong reliance on the information mechanism coincides with the interviewed lawyers' answer to the question of what was their main reason to apply for an EAPO. Five out of eight Spanish lawyers mentioned that the information mechanism was their only reason to use the EAPO Regulation. They put more emphasis on the possibility of finding out whether they could discover if the debtor had assets abroad rather than on achieving temporary attachment of the bank accounts.

With the exception of Germany, from the side of the information authorities the number of information request has been limited. By May 2020, the German information authority received 113 requests.⁵⁸ Conversely, between 2017 and 2020, the Luxembourgish information authority received just 29 requests,⁵⁹ while its Spanish counterpart just 20.⁶⁰

⁵² Statistisches Bundesamt, Fachserie 10 Reihe 2.1, Rechtspflege Zivilgerichte 2020 (2021), available at: <<https://www.destatis.de/DE/Themen/Staat/Justiz-Rechtspflege/Publikationen/Downloads-Gerichte/zivilgerichte-2100210207004.html>> (accessed on 15 November 2021).

⁵³ Parquet général du Grand-Duché de Luxembourg, *Rapports juridictions judiciaires 2020* (2021), available at: <<https://justice.public.lu/fr/publications/juridictions-judiciaires/rapports-juridictions-judiciaires-2020.html>> (accessed on 15 November 2021), p. 64.

⁵⁴ See:

<<https://www6.poderjudicial.es/PXWeb2021v1/pxweb/es/10.Juzgados%20de%20Primera%20Instancia%20e%20Instrucci%3b3n/-/OUJII049.px/table/tableViewLayout1/>> (accessed on 15 November 2021).

⁵⁵ Between 2020 and 2021, a total of 46 interviews were conducted with judges, court clerks, bailiffs, lawyers and information authorities.

⁵⁶ However, in 2020, according to the official statistics of the Parquet général only 6 out of the 19 EAPO applications included a request for information: Parquet général du Grand-Duché de Luxembourg, *Rapports juridictions judiciaires 2020* (2021), available at: <<https://justice.public.lu/fr/publications/juridictions-judiciaires/rapports-juridictions-judiciaires-2020.html>> (accessed on 15 November 2021), p. 64.

⁵⁷ In Spain, information requests were contained in 22 out of 32 identified EAPO applications; while in Germany, they were eight out of the 18 applications.

⁵⁸ Email from the German information authority received on 6 May 2020 (on file with author).

⁵⁹ Answer to the questionnaire received from the Luxembourgish information authority received on 14 May 2021 (on file with author).

⁶⁰ Answers to the questionnaire received from the Spanish information authority received on 9 December 2020 (on file with author).

II. A fragmented application

The wide margin of appreciation left to Member States to implement the information mechanism is a source of divergences in the manner this is applied at the domestic level. Some information authorities charge fees and others do not.⁶¹ The use of different methods to retrieve information also affects the time required to provide the court of origin with an answer. The two or three days that it takes for the German information authority to obtain the information⁶² contrasts with the more than three weeks that the Luxembourgish information authority needs to reply.⁶³ The reason it takes much longer in Luxembourg is that information about the bank accounts is obtained by asking all the banks in that country to disclose if they hold the debtor's bank accounts.⁶⁴ Banks have twenty days to provide the information authority with an answer.⁶⁵

Even in some aspects expected to be applied uniformly, one can find differences. For instance, in Spain, some courts do not require the claimant to prove the *periculum in mora* before sending the request for information.⁶⁶ For these courts, the existence of an enforceable title and the absence of assets in Spain was sufficient to justify the use of the information mechanism. Conversely, in Germany and Lithuania, courts refused to send an information request because they considered that claimants had not properly justified the *periculum in mora*.⁶⁷ Information authorities even apply different standards of protection of the debtor's personal data. The German information authority follows a strict application of the principle of data minimization, providing only the name and address of the bank or banks which hold the debtor's bank accounts.⁶⁸ However, one Spanish court which sent a request to Portugal also received account balances.⁶⁹ Since there were no funds, the creditor decided to withdraw the EAPO application.

⁶¹ Art. 49 EAPO Regulation.

⁶² Interview with a Luxembourgish judge held on 4 February 2019 (notes on file with the author).

⁶³ Answers to the questionnaire sent to the Luxembourgish information authority received on (on file with the author).

⁶⁴ Art. 2(6) Amended law of 23 December 1998 establishing a supervisory commission for the financial sector (*Loi modifiée du 23 décembre 1998 portant création d'une commission de surveillance du secteur financier*).

⁶⁵ Veerle Van Den Eeckhout and Carlos Santaló Goris, 'Luxembourg' in Jan von Hein and Thalia Kruger (eds.), *Informed Choices in Cross-Border Enforcement. The European State of the Art and Future Perspectives* (Intersentia 2021), p. 295.

⁶⁶ Interview with a Spanish court clerk held on 2 February 2021 (notes on file with the author); Interview with a Spanish court clerk held on 27 July 2021 (notes on file with the author); Interview with a Spanish court clerk held on 10 September 2021 (notes on file with the author).

⁶⁷ Germany: OLG Hamm 8 Zivilsenat 14.01.2019 I-8 W 51/18 8 W 51/18 ECLI:DE:OLGHAM:2019:0114.8W51.18.00; Lithuania: Kauno apygardos teismas 2018-01-30 Byla E2S-362-413/2018; Šiauliai District Court 11/9/2018 E2-15962-650/2018; Vilniaus apygardos teismas 2019-01-10 Byla 2S-49-431/2019; Vilniaus apygardos teismas 2019-01-17 Byla 2S-65-653/2019; Utenos apylinkės teismas 2019-01-22 Byla E2VP-216-477/2019.

⁶⁸ Interview with a Spanish court clerk held on 8 September 2021 (notes on file with the author).

⁶⁹ Interview with a Spanish court clerk held on 27 July 2021 (notes on file with the author).

III. Issues detected in the practice

Court practice has brought to light problems and difficulties experienced by them with the information mechanism. Some of these problems derive from how the European legislator conceived this information mechanism, while others find their origin in its implementation at the national level.

a. Lack of an adequate design of the information mechanism for cross-border dialogue

The information mechanism was primarily conceived for the exchange of information between courts and information authorities located in different Member States. However, Article 14 omits some basic necessary aspects/elements that assure good cross-border communication. This provision is silent on the content of the request for information submitted by the court of origin; or the answer to be provided by the information authority. Neither is there a standard form for the courts to submit the request.⁷⁰ Such omissions undermine a proper dialogue between courts and authorities.⁷¹ For instance, a Spanish court found its request for information in Germany rejected, because the German information authority considered that information provided was insufficient to justify that the debtor could have bank accounts in Germany.⁷² Had the EAPO Regulation clarified the content of the information request, such a situation would not have happened. The European legislator should have also required the Member States to appoint central bodies as information authorities. As the CJEU has acknowledged,⁷³ having a central body helps in terms of specialization in EU law. In France, any of its more than 3,000 bailiffs can act as an information authority.⁷⁴ One Luxembourgish judge, who had asked for information about the debtor's possible bank accounts in France, found that the bailiff was completely unaware of the EAPO or its information mechanism.⁷⁵ This contrasts with Germany or Spain, both having relied on domestic bodies with long-standing experience in the field of cross-border judicial cooperation. In Germany, the information authority is Federal Office of Justice (*Bundesamt für*

⁷⁰ However, in 2020, the European Judicial Network created an *ad hoc* unofficial standard form for courts to submit the request for information. This non-mandatory standard form was made available on the ejustice portal: < https://e-justice.europa.eu/378/EN/european_account_preservation_order_forms?clang=en > (accessed on 29 November 2021).

⁷¹ Noemie Reichling, *Les principes directeurs du procès civil dans l'Espace judiciaire européen* (2017), available at: <<https://tel.archives-ouvertes.fr/tel-01802966>> (accessed on 29 November 2021), para. 245.

⁷² Interview with a Spanish judge held on December 2020 (notes on file with author).

⁷³ Joined Cases, C-400/13 and C-408/13, 18 December 2014, *Sanders and Huber*, EU:C:2014:246CJEU, para. 44; C-30/20, 15 July 2021, *Volvo*, ECLI:EU:C:2021:604, para. 37.

⁷⁴ European Judicial Atlas - European Account Preservation Order - France: < https://e-justice.europa.eu/379/EN/european_account_preservation_order?FRANCE&member=1 > (accessed on 29 November 2021).

⁷⁵ Veerle Van Den Eeckhout and Carlos Santaló Goris, 'France' in Jan von Hein and Thalia Kruger (eds.), *Informed Choices in Cross-Border Enforcement. The European State of the Art and Future Perspectives* (Intersentia 2021), p. 206.

Justiz);⁷⁶ while in Spain, it is the Subdirectorate General for International Judicial Cooperation (*Subdirección General de Cooperación Jurídica Internacional*).⁷⁷

b. Lack of adequate national implementation

A second set of problems are caused by the lack of proper implementation of the information mechanism at the domestic level. The EAPO Regulation was immediately applicable from the moment it entered into force. Nevertheless, due to the number of references to the national laws of the Member States, some sort of national legislative implementation could be expected.⁷⁸ All Member States except Portugal have approved specific legislative acts concerning the EAPO Regulation, though their content and extent vary substantially from one Member State to another. Furthermore, some were approved after the EAPO had entered into force. As a result, certain Member States were less prepared than others to ensure adequate functioning of the information mechanism. For instance, during the EAPO Regulation's first year in force, the Spanish information authority lacked specific powers to retrieve information about debtors' bank accounts.⁷⁹ The same happened in Belgium, where, initially, its information authority had to reject information requests because it did not have the technical means to search bank accounts.⁸⁰ Italy only approved the EAPO implementing legislation in 2020.⁸¹ Perhaps, the most manifest case was Romania, which until January 2020 did not appoint an information authority.⁸² Against this backdrop, a Spanish court required the assistance of the European Judicial Network to find a way to obtain information about bank accounts that a debtor had in Romania.⁸³

National implementation also encompasses preparing domestic authorities to deal with the EAPO. The lack of awareness about the EAPO can also lead to disruptions

⁷⁶ Art. 948(1) German Code of Civil Procedure (*Zivilprozessordnung*).

⁷⁷ European Judicial Atlas - European Account Preservation Order - Spain: < https://ejustice.europa.eu/379/EN/european_account_preservation_order?SPAIN&member=1#a_88 > (accessed on 29 November 2021).

⁷⁸ In this regard, Gascón Inchausti refers to this kind of instrument as “directive-regulations” (*reglamentos directivos*) implying a need for a legislative action from the Member States: Fernando Gascón Inchausti, *Derecho europeo y legislación procesal civil nacional: entre autonomía y armonización* (Marcial Pons 2018).

⁷⁹ Paula Monge Royo, “Circulation and enforcement of decisions: the role of international cooperation” (Workshop: Circulation and enforcement of foreign decisions involving pecuniary debts: the Spanish experience, University Complutense of Madrid, Spain, 10 October 2019).

⁸⁰ Answer to the questionnaire about the information mechanism provided by the Belgian National Chamber of Bailiffs (*Chambre nationale des huissiers de justice*) received 13 June 2019 (on file with author).

⁸¹ Art. 3(3) Legislative Decree No. 152/2020 (*Decreto Legislativo No. 152/2020*).

⁸² And only after the European Commission had taken the first preliminary step of an infringement proceeding against Romania. One of the reasons was, precisely, the lack of implementation of the EAPO information mechanism. See: Elena Alina Onțanu, “From Direct Application of European Uniform Procedures to Implementation Legislation in Romania” available at: <https://eapil.org/2020/11/19/from-direct-application-of-european-uniform-procedures-to-implementation-legislation-in-romania/> (accessed on 15 November 2021).

⁸³ Francisco Javier Forcada Miranda, “Circulation and enforcement of decisions: a view from the Spanish courts” (Workshop: Circulation and enforcement of foreign decisions involving pecuniary debts: the Spanish experience, University Complutense of Madrid, Spain, 10 October 2019).

in its application. One good example of this phenomenon is offered by the case of the already mentioned French bailiff who did not know how to react to a petition of information because he was unaware of the existence of the EAPO Regulation.⁸⁴ Another example is offered by the case of the Spanish court which rendered an EAPO without any information about the bank accounts. The court expected that the authorities in the Member State of enforcement would find them.⁸⁵ Had the French bailiff and the Spanish judge received proper training about the EAPO Regulation, those situations would not have occurred.

Concluding Remarks and Outlook

By 17 January 2022, the Commission is scheduled to issue a report on the application of the EAPO Regulation.⁸⁶ This report could be accompanied by “a proposal to amend this Regulation and an assessment of the impact of the amendments to be introduced”.⁸⁷ This date coincides with the fifth anniversary of the EAPO Regulation, and thus, of the information mechanism. During these five years in force, the information mechanism has been one of the main drivers for creditors to trust the EAPO proceeding before German, Luxembourgish, and Spanish courts. On the less bright side, this period has served to detect issues on the functioning of the information mechanism and prove that there is still room for improvement. Some of these problems are caused by the courts and authorities’ lack of experience with the EAPO,⁸⁸ while others are rather structural and might require amendments. Creating mandatory central information authorities or setting up uniform standard forms are just some examples of improvements that would facilitate its application. Considering the low numbers of EAPOs, its reform in the foreseeable future should not be ruled out. The European Small Claims Procedure’s underperformance was one the reasons that triggered its reform,⁸⁹ which occurred only seven years after the Regulation entered in force.⁹⁰ If the Commission ultimately decides to recast the

⁸⁴ Veerle Van Den Eeckhout and Carlos Santaló Goris, “France” in Jan von Hein and Thalia Kruger (eds.), *Informed Choices in Cross-Border Enforcement. The European State of the Art and Future Perspectives* (Intersentia 2021), p. 206.

⁸⁵ Interview with a Spanish lawyer held on 10 February 2021 (notes on file with the author).

⁸⁶ Art. 53(1) EAPO Regulation.

⁸⁷ Art. 53(1) EAPO Regulation.

⁸⁸ In this sense: Burkhard Hess, “The Effective Disclosure of the Debtor’s Assets in Enforcement Proceedings” in Masahisa Deguchi (ed.), *Effective Enforcement of Creditors’ Rights* (Springer 2022), p. 40.

⁸⁹ Regulation (EU) 2015/2421 of the European Parliament and of the Council of 16 December 2015 amending Regulation (EC) No 861/2007 establishing a European Small Claims Procedure and Regulation (EC) No 1896/2006 creating a European order for payment procedure, OJ L 341, 24.12.2015, p. 1-13.

⁹⁰ Cristian Oró Martínez, “The Small Claims Regulation: On the Way to an Improved European Procedure?” in Burkhard Hess, Maria Bergström and Eva Storskrubb (eds.), *EU Civil Justice: Current Issues and Future Outlook* (Bloomsbury 2015), pp. 124-125.

EAPO Regulation, one may hope that such reform brings forth the necessary amendments to achieve a more efficient and effective information mechanism.

About the Author



Carlos Santaló Goris is a research fellow at the Max Planck Institute for International, European and Regulatory Procedural Law. He studied at the University of Santiago de Compostela and the University of Fribourg (ERASMUS), obtaining his diploma in 2014. He pursued postgraduate studies at the University of Saarland (LL.M. program in European and International Law) and the University of Luxembourg (LL.M. program in European Economic and Financial Criminal Law).

Before joining the MPI as a Research Fellow, he worked as a junior legal officer in a multinational financial services firm in Luxembourg. He is a Ph.D. candidate at the University of Luxembourg, writing a thesis about the enforcement of the European Account Preservation Order Regulation in Germany, Luxembourg, and Spain under the supervision of Professor Burkhard Hess from the University of Heidelberg.

Contact Carlos Santaló Goris: carlos.santalo@mpi.lu

The Financial Conduct Authority and NatWest Bank

Professor Stuart Bazley

Introduction

Amongst the UK Financial Conduct Authority's (FCA or Authority) enforcement activity during 2021, the criminal prosecution of NatWest Bank plc (NatWest and the Bank) for offences contrary to certain obligations set out in the Money Laundering Regulations 2007, may be regarded as one of the most notable FCA enforcement cases of 2021. The circumstances and facts of the case are complex, but this article considers in outline, aspects of the background to the prosecution and some of the relevant regulatory provisions, that may be of interest to those readers working in or researching anti-money laundering law and compliance.

An outline of the framework of Anti-Money Laundering law

Before considering the FCA NatWest prosecution, it may be helpful to consider the framework of law and regulation currently governing money laundering in the United Kingdom as well as aspects of the law in force and applicable to the circumstances of the NatWest case. The law is comprised of primary legislation set out in the Proceeds of Crime Act 2002, which describes amongst other things, offences related to the laundering of the proceeds of crime; Secondary legislation in the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017¹ (the 2017 Regulations), which came into force on 26 June 2017, applying to 'Relevant Persons' as defined in regulation 8, which include a range of activities, such as that of, credit institutions, financial institutions, independent legal professionals and trust and company service providers. The 2017 Regulations in particular set out the arrangements Relevant Persons need to have in place to guard against the risk of their business being used to launder the proceeds of crime, along with provisions setting out supervisory and enforcement mechanisms. Prior to 26

¹ The 2017 Regulations was amended by the Money Laundering and Terrorist Financing (Amendment) Regulations 2019)

June 2017, The Money Laundering Regulations 2007 (2007 Regulations) provided for the range of arrangements that Relevant Persons as defined in the 2007 Regulations were required to establish. Regulation 45 (1) of the 2007 Regulations provided that a contravention of certain requirements in the regulations was a criminal offence. It will be seen later in this article that the prosecution of NatWest bank was in relation to certain contraventions of the 2007 Regulations. A third limb of the framework of regulation, in the 2017 Regulations and previously the 2007 Regulations is the role played by certain relevant and approved guidance, the following of which is to be considered in determining whether a Relevant Person has complied with the law. By way of example, regulation 45 of the 2007 Regulations provided:

'...(2) In deciding whether a person has committed an offence under paragraph (1), the court must consider whether he followed any relevant guidance which was at the time—

(a) issued by a supervisory authority or any other appropriate body;

(b) approved by the Treasury; and

(c) published in a manner approved by the Treasury as suitable in their opinion to bring the guidance to the attention of persons likely to be affected by it.'

The UK Joint Money Laundering Steering Group publishes guidance for certain firms that its member bodies represent and which are regulated by the Financial Conduct Authority.²

The significance of compliance with anti-money laundering law by firms regulated by the Financial Conduct Authority and the importance of robust system of control, is often stressed by the Authority for instance in April 2021, Mark Steward the FCA's Executive Director of Enforcement and Market Oversight, commented on the need for anti-money laundering controls stating:

'Systems and controls that are purposeful, efficient and courageous in identifying suspicious activity are vitally important; system and control failures, on the other hand, provide an invisible, illicit cover for criminals and

² See the Joint Money Laundering Steering Group. Guidance. <https://www.jmlsg.org.uk/guidance/current-guidance>. Accessed 24 January 2022. The Financial Conduct Authority also now publishes in its Financial Crimes Guide certain 'relevant guidance' on money laundering, the FCA's guidance is not however approved by HM Treasury. See the Financial Conduct Authority Financial Crimes Guide, Chapter 3 'FCG3, Money Laundering and Terrorist Financing'. <https://www.handbook.fca.org.uk/handbook/FCG/3/?view=chapter>. Accessed 3 February 2022.

*criminal activity that affects the whole community, not only in this country but also beyond, and can erode confidence in the financial system*³

The NatWest Bank Plc prosecution

The FCA has a range of powers available if it wishes to take enforcement action against a firm it regulates for breaches of anti-money laundering requirements. As noted above, Regulation 86 (1) of the 2017 Regulations and previously 45(1) of the 2007 Regulations provide that it is a criminal offence to fail to comply with certain obligations in the respective regulations.

The FCA's prosecution of NatWest Bank Plc is significant for being the Authority's first prosecution under the 2007 Regulations. The prosecution related to three offences under the 2007 Regulations;⁴ being failures to comply with requirements relating to risk sensitive due diligence and on-going monitoring as set out in Regulations 8(1), 8(3) and 14(1). The regulations in question provided as follows:

- 1) Regulation 8(1) 'A relevant person must conduct ongoing monitoring of a business relationship' (the statement of Agreed Facts published in the case, which is further referred to below⁵, states that the Bank failed to meet this obligation between 7 November 2013 and 23 June 2016);
- 2) Regulation 8(3) as applied by regulation 7(3) (a) being to, conduct ongoing monitoring on '...a risk sensitive basis and 7(3)(b) 'demonstrate to his supervisory authority that the measures is appropriate in view of the risks of money laundering...' (the statement of Agreed Facts states that the Bank failed to meet this obligation between 8 November 2012 and 23 June 2016), and;
- 3) Regulation 14(1) 'A relevant person must apply on a risk sensitive basis enhance due diligence measures and enhanced monitoring (the statement of

³ The Financial Conduct Authority. 'The Importance of purposeful anti-money Laundering Controls' Speech by Mark Steward, Executive Director of Enforcement and market Oversight at the AML & ABC Forum 2021. 1 April 2021. <https://www.fca.org.uk/news/speeches/importance-purposeful-anti-money-laundering-controls>. Accessed 23 January 2022

⁴ The Money Laundering Regulations 2007 were applicable to facts of the Nat West prosecution. New regulations came into force on 26 June 2017 which are set out in The Money laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017

⁵ R (The Financial Conduct Authority) v National Westminster Bank Agreed Statement of Facts <https://www.fca.org.uk/publication/corporate/agreed-statement-facts-fca-national-westminster-bank.pdf>. Accessed 23 January 2022

Agreed Facts states that the bank failed to meet this obligation between 8 November 2012 and 23 June 2016).

But aside from specific offences charged, material published in the case, including an Agreed Statement of Facts prepared by the prosecution and NatWest Bank⁶ and the sentencing judges remarks about the regulations⁷, provides a useful insight into the 2007 regulations and how weaknesses can arise in money laundering systems of control.

The case was concerned with the Bank's business relationship with a customer named Fowler Oldfield, which ran a jewellery business. In short, the customer's business with NatWest was not consistent with what the Bank had understood initially it would be. As will be revealed below, many of the banking transactions that took place, involved the deposits of large volumes of cash, and Fowler Oldfield was subject to a police investigation relating to offences for money laundering. Providing a sense of the scale of the Fowler Oldfields activity at the bank, when announcing the charges against NatWest, the FCA stated: *'The case arises from the handling of funds deposited into accounts operated by a UK incorporated customer of NatWest. The FCA alleges that increasingly large cash deposits were made into the customer's accounts. It is alleged that around £365 million was paid into the customer's accounts, of which around £264 million was in cash... 'It is alleged that NatWest's systems and controls failed to adequately monitor and scrutinise this activity.'*⁸

Anti-Money Laundering and monitoring

The 2021 prosecution of NatWest was concerned with offences related to weaknesses in the Bank's monitoring of its customer's business and whether those weaknesses, in the context of the customer's business undertaken with the Bank, meant the Bank had not met relevant regulations. To provide an insight into the nature of the identified weaknesses, the FCA in a press release stated that:

'Some of the bank's employees, who were responsible for handling these cash deposits, reported their suspicions to bank staff responsible for investigating suspected money laundering, however no appropriate action was ever taken. The

⁶ n5.

⁷ Judiciary of England and Wales, R(The Financial Conduct Authority) v National Westminster Bank PLC 'Sentencing remarks' of Mrs Justice Cockerill 13 December 2021. <https://www.judiciary.uk/wp-content/uploads/2021/12/FCA-v-Natwest-Sentencing-remarks-131221.pdf>. Accessed 1 January 2022.

⁸ The Financial Conduct Authority. Press release 'FCA starts criminal proceedings against NatWest Plc' 16 March 2021 <https://www.fca.org.uk/news/press-releases/fca-starts-criminal-proceedings-against-natwest-plc>. Accessed 24 January 2022.

‘red flags’ that were reported included significant amounts of Scottish bank notes deposited throughout England, deposits of notes carrying a prominent musty smell, and individuals acting suspiciously when depositing cash in NatWest branches. In addition, the bank’s automated transaction monitoring system incorrectly recognised some cash deposits as cheque deposits. As cheques carry a lower money laundering risk than cash, this was a significant gap in the bank’s monitoring of a large number of customers depositing cash, of which Fowler Oldfield was one.’⁹

Mrs Justice Cockerill’s (the sentencing Judge in the case) remarks¹⁰ illuminated some of the risk associated with cash deposit business and the expectations of the JMLSG guidance, stating in particular:

‘All banks operating in the retail banking space have had it clearly flagged to them by the JMLSG that the provision of services to cash- generating businesses is a particular area of risk, and that there is a corresponding need for careful assessment of that risk. It is incumbent upon corporate entities in such positions to justify their position by a scrupulous regard both for establishing and carefully operating systems which will prevent the infiltration of the financial sector by money which is the proceeds of crime and will also ensure that those who seek to do so are not allowed to flourish.’¹¹ and;

‘...Moreover, it must be borne in mind that although in no way complicit in the money laundering which took place, the Bank was functionally vital. Without the Bank - and without the Bank’s failures - the money could not be effectively laundered.’¹²

During the period relevant to the offences, the Bank did of course operate anti-money laundering systems of control. The sentencing Judge remarked on the Bank’s approach to compliance with the 2007 Regulations and the Bank’s use of a ‘Three Lines of defence’ model, and its various constituents; with first line arrangements including: ‘manual monitoring of transactions by staff...’; ‘monitoring by members

⁹ The Financial Conduct Authority. Press release ‘NatWest fined £264.8million for anti-money laundering’ 13 December 2021 <https://www.fca.org.uk/news/press-releases/natwest-fined-264.8million-anti-money-laundering-failures>. Accessed 24 January 2022.

¹⁰ Judiciary of England and Wales, R(The Financial Conduct Authority) v National Westminster Bank PLC ‘Sentencing remarks’ of Mrs Justice Cockerill 13 December 2021. <https://www.judiciary.uk/wp-content/uploads/2021/12/FCA-v-Natwest-Sentencing-remarks-131221.pdf>. Accessed 1 January 2022.

¹¹ n10 Para 122.

¹² n10 Para 123.

of the relationship management team...’; ‘General Staff vigilance...’; and ‘review of customer accounts on a periodic basis...’, ‘automated monitoring of transactions...’ and ‘investigations of activity identified as unusual/suspicious by automated/manual monitoring’.¹³

The sentencing Judge goes on to remark on weaknesses identified in the Bank’s monitoring, including its monitoring of the Fowler Oldfield account and the Bank’s automated transaction monitoring system. In particular, and with reference to the cash deposits, the Judge noted:

‘Throughout the Indictment Period, cash deposits made directly through Bank cash centres were erroneously interpreted by the system as cheque deposits. Although they were subject to the Security Blanket (as defined below), those cash deposits were not subjected to cash-specific monitoring rules. Instead, they were subjected to less stringent rules applicable to cheque deposits (when such rules existed).’¹⁴ And; ‘For most of NatWest’s relationship with Fowler Oldfield, there were no cheque-specific monitoring rules in place. Those deposits by Fowler Oldfield made through Bank cash centres amounted to millions of pounds in cash that were neither monitored as cash nor subjected to rules specifically targeting cheque deposits’.¹⁵

The case resulted in the Bank’s guilty plea and the imposition of a criminal fine of just over £264.7m. Mark Steward, the FCA’s Executive director of Enforcement and Market Oversight, commenting on the case referred to the extent of the weakness in the Bank’s controls, in the context of the cash deposits made, stating: *‘NatWest is responsible for a catalogue of failures in the way it monitored and scrutinised transactions that were self-evidently suspicious. Combined with serious systems failures, like the treatment of cash deposits as cheques, these failures created an open door for money laundering’¹⁶*

Additionally, Mr Steward put the prosecution into the context of the role played by, and impact of, effective anti-money laundering compliance, stating: *‘Anti-money*

¹³ n10 para 13. For further information on ‘Three Lines of defence model’ See The Chartered Institute of Internal Auditors. Policy Paper ‘Internal audit, risk and corporate governance - the Three Lines of Defence Model’ March 2015 <https://www.iaa.org.uk/media/1042665/three-lines-of-defence-march-2015.pdf>. Accessed 24 January 2022.

¹⁴ n10 para 17 (a)

¹⁵ n10 para 17 (b).

¹⁶ The Financial Conduct Authority, Press release ‘Nat West fined £264.8 million for anti-money laundering failures’ 13 December 2021. <https://www.fca.org.uk/news/press-releases/natwest-fined-264.8million-anti-money-laundering-failures>. Accessed 14 December 2021.

*laundering controls are a vital part of the fight against serious crime, like drug trafficking, and such failures are intolerable ones that let down the whole community, which, in this case, justified the FCA's first criminal prosecution under the Money Laundering Regulations.'*¹⁷

A careful analysis of the Agreed Facts and Sentencing Judge's remarks can provide useful information for the financial services sector, insight into some of the risks that can be present in certain types of business activity, and the need to devise and operate effective systems of control. The current 2017 Regulations and previously the 2007 Regulations, set out the regulatory requirements for persons within their scope, including the need to establish appropriate risk focused systems of monitoring and customer due diligence. Furthermore, guidance for relevant UK firms on how to approach compliance with the regulations is provided by the JMLSG and the FCA.¹⁸ It is perhaps helpful to conclude with a quote addressing the purpose of the Money Laundering Regulations from Mark Steward, the FCA's Executive Director of Enforcement and Market Oversight:

*'We know much of the industry is devoted to strong systems and controls in relation to AML. Indeed, the aim of AML regulation is not to catch anyone out but to set high standards of probity and scrutiny to inhibit illicit money flows in the financial system and to encourage participants in the system to behave as custodians and guardians of the public interest in preventing money laundering.'*¹⁹

About the Author

Stuart Bazley is a Visiting Professor in Financial Regulation and Compliance Law 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.

¹⁷ n16.

¹⁸ n2 .

¹⁹ n3.

Strategic Partners



Clarity in a complex world



Grant Thornton

An instinct for growth™



serle court





Connect with ICC FraudNet

ICC Commercial Crime Services
ICC FraudNet
Cinnabar Wharf
26 Wapping High Street
London
E1W 1NG
United Kingdom
Phone: +44 (0)20 7423 6960
Fax: +44 (0)20 7423 6961
fraudnet@icc-ccs.org
www.iccfraudnet.org
www.icc-ccs.org

