

ICC FraudNet
Global Annual Report 2025

THE STATE OF FRAUD AND ASSET RECOVERY: TIMELESS CRIMES, MODERN APPROACHES

**EDITED BY
DR DOMINIC THOMAS-JAMES**

ICC FraudNet Global Annual Report 2025

Published by ICC FraudNet in 2025 on www.iccfraudnet.org.

©2025 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 2025 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.

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

www.iccfraudnet.org

About ICC FraudNet

ICC FraudNet was founded in 2004 by several leading asset recovery lawyers in collaboration with ICC Commercial Crime Services, the anti-crime arm of the Paris based International Chamber of Commerce.

ICC FraudNet is an international network of independent lawyers who are the leading civil asset recovery specialists in their country. Using sophisticated investigation and forensic tools and cutting-edge civil procedures, ICC 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, crypto and bankruptcy & insolvency.

Acknowledgments

The Editor wishes to acknowledge the following individuals who have been of great support and valued assistance in the publication of the 5th ICC FraudNet Global Annual Report. First, a special thanks goes to Nicola Stenhouse, Executive Secretary of ICC FraudNet who has provided great support and enthusiasm for this initiative. In her inaugural year at the helm of this international network, Nicola has not only been of significant logistical assistance – but has so powerfully advocated the value of this practitioner resource in international fora.

The Editor also wishes to thank Mr Peter Lowe, former Executive Secretary of ICC FraudNet for his steadfast support of this initiative from its conception 5 editions ago! Thanks also go to FraudNet’s Co-Executive Chairs and Directors, Aimee Prieto of Prieto Cabrera & Asociados, S.R.L., Dominican Republic, and Danny Ong of Seita Law LLC, Singapore for their continued support in the preparation of this report.

To the authors of the 2025 Global Annual Report: your thought leadership and unique perspectives contained in this publication make it the valued research and practical resource it is. This contribution to knowledge in such a dynamic area of law, serves as a tool both within ICC FraudNet and to the Report’s global readership. It is a privilege to have worked with each of you and your colleagues on this Report.

The Editor also wishes to acknowledge the authors’ staff for their support and liaison during the research, writing and editing stages of submissions.

I also wish to thank and note the work of ICC FraudNet’s Director of Marketing and Communications, Priya Jethwa for her promotional efforts and assistance in the preparation of the 2025 Report and her great work in promoting it to a global audience.

Finally, gratitude goes to ICC Commercial Crime Services and the ICC FraudNet staff for their support of this initiative.

Editor's Summary

Dr Dominic Thomas-James
Editor, ICC FraudNet Global Annual Report




It is my pleasure to welcome readers to the 2025 ICC FraudNet Global Annual Report on Fraud and Asset Recovery. The ICC FraudNet Global Annual Report, now in its Fifth Edition, takes as its theme The State of Fraud and Asset Recovery: Timeless Crimes, Modern Approaches. It builds on the previous four editions of the Global Annual Report and expands ICC FraudNet's growing body of thought-leadership, practitioner and scholarly insights.

While many readers are well acquainted with our work – for those unfamiliar, ICC FraudNet is the world's leading fraud and asset recovery lawyers' network with a membership spanning all corners of the globe. Members and Strategic Partners are routinely involved in some of the most high-profile, sensitive, complex and impactful fraud and asset recovery cases. Their perspectives in these pages make for fascinating and original reading.

Of course, 2025 as a backdrop to these contributions continues to present a world of challenges including conflict, economic hardship, political instability and social volatility. Financially acquisitive crimes like bribery, fraud, theft and money laundering continue to expand in scope and impact. The contributions in this Report endeavour to explain the incidence of such criminality, consider practical approaches within the law and investigations sectors to pursue, interdict and disrupt fraud and financial crime, while providing practical observations, expert insight and messages of caution to those interested in our field. The articles here provide expert observations on current and recent fraud cases, and thoughtful reflections on asset recovery investigations. From paper trails and ledgers, to learning models and dynamic technologies – the articles in this Report consider fraud and recovery from numerous approaches.

The themes and subjects addressed in this Report are vast and often overlapping, including: cyber-crime and ransomware attacks, corporate transparency and beneficial ownership information, looted state property and its recovery, crypto compliance, cyber-security challenges, foreign judgment enforcements, jurisdiction-specific arbitration, trends in investigations such as Large Language Models, the impact of AI and AI-decision making in litigation and investigations, the relationship




between equitable liens and fraud, exploration of different cash-tracing methodologies, the role and rationale of the financial regulator, offshore considerations, encrypted messaging applications and their challenges for investigators, recovering funds from complex banking chains, corruption and fraud, civil and criminal law mechanisms for asset recovery, and the manipulation risks presented by AI.

One of the resounding themes this year has certainly been the development of technology, its impact on fraud, its positive uses and negative risk-factors in terms of fraud as well as investigations, and warnings for future development, regulation and use. This is particularly visible in those papers which explore the increasingly potent role of AI – in some instances pointing to the pace at which it is simultaneously assisting fraud investigations, but also challenging them. Tales of caution about AI's ability as a manipulator, as well as encouragement as to its helpful role in investigations, as well as its competence, or otherwise, in serving as a decision-maker, are all considered in the Report.

As ever, jurisdiction representation in the Report is very strong – with original insights coming from leading lawyers and investigators in the U.K., U.S., Spain, Hungary, Ghana, Poland, Panama, Cayman Islands, New Zealand, Guernsey, Japan, the British Virgin Islands, China, Singapore and South Africa. The 23 original papers have been authored by some 37 authors.

Set against members' and strategic partners' busy workloads, our authors have, yet again, found time to write thought-provoking articles and thereby contribute their expertise to a wide readership through this publication. It is not only about showcasing the work that ICC FraudNet does as a network: but it is about contributing knowledge to important and ever-developing subject areas in which meaningful expertise is much needed. In an age of increasing content and sound-bite knowledge; these papers represent thoroughly researched and thoughtfully considered approaches to important legal issues.



Since Covid-19, the relationship between volatility and fraud continues to be more relevant than ever. In the UK, as it is suspected in many other jurisdictions in which readers of this publication practise or live, fraud in today's age is said to be the crime to which we are all most likely to fall victim. While keeping valuables out of sight of thieves has, perhaps, become common sense for many – fraud continues to perplex us for many reasons. It follows that if our understandings of fraud were so advanced, then surely it wouldn't be the most likely crime we may fall victim to. As one author aptly notes in the coming pages, trust cannot be broken unless it is first given. As such, the stakes could not be higher.

The individually authored papers in this Report aim to offer practical and relevant perspectives on these important issues. Not only do we hope they are of use to the wider ICC FraudNet and ICC Networks, Strategic Partners and other professional collaborators, but also to clients and prospective clients. Further, it is hoped that the papers are of relevance to a wider audience including lawyers, investigators, enforcement and regulatory professionals, in-house compliance teams, policymakers and lawmakers, academicians and researchers alike. Ultimately, the papers draw upon collective and individual experiences, best practices and case studies seen at the cutting edge of the field. It is hoped that the compendium of papers offer real-world solutions and expert insights to tackle fraud and acquisitive misconduct, while offering support and practicality in terms of the challenges of international asset recovery efforts across different jurisdictions in responding to fraud. In doing so, the Report aims to support the reader's understanding and knowledge in what is an increasingly complex subject.

It is hoped that the 2025 Report, like its previous editions, continues to serve as a useful research and practice resource for those interested in the field of asset recovery and fraud.

Dr Dominic Thomas-James
Editor, ICC FraudNet Global Annual Report

Executive Secretary's Foreword

Nicola Stenhouse
Executive Secretary, ICC FraudNet



As the new Executive Secretary of ICC FraudNet, I am pleased to introduce the 2025 Global Annual Report, a collaborative effort authored by our distinguished members, Strategic Partners, and friends of the network.

In a time marked by geopolitical uncertainty and rapid technological advancement, this year's report provides a unique, cross-jurisdictional perspective on the most pressing issues confronting the asset recovery community. The breadth and depth of these contributions reaffirm that, despite the growing complexity and sophistication of global fraud, our community is not only adapting, but advancing. Sharing insights through networks, conferences, and publications such as this, remains essential to staying ahead and going further, faster.

Many readers will already be familiar with the authors of these articles who are leading practitioners and thought leaders in their respective domains. We are fortunate to benefit from their expertise, and I am deeply grateful to each of them for contributing their time and insight to this volume. Their work helps to ensure that ICC FraudNet remains at the cutting edge of global asset recovery practice.

This year's Global Annual Report is structured around five key themes:

- I. Perspectives on AI
- II. Enforcement and Regulation
- III. Asset Recovery Investigations: Criminal, Civil, and Technological Perspectives
- IV. Cybercrime
- V. Tackling Fraud, Corruption, and Money Laundering
- VI. Practical Perspectives

Each part offers not only thoughtful analysis but also practical tools and strategies to navigate today's complex landscape.

I encourage readers, whether lawyers, academics, practitioners, or students, to engage deeply with the material. May it provoke new ideas, foster collaboration, and inspire ongoing excellence in the pursuit of justice and the recovery of stolen assets.

Nicola Stenhouse
Executive Secretary, ICC FraudNet

Contents

About ICC FraudNet	iii
Acknowledgments	iv
Editor's Summary Dr Dominic Thomas-James	v
Executive Secretary's Foreword Nicola Stenhouse	viii
Authors	xii
Part 1: Current Perspectives on Artificial Intelligence	1
Breaking the Iron Triangle? The Future of AI Decision Making in Litigation Nick Dunne	2
Staying a Step Ahead of Fraudsters in the Age of AI Brooke Berg, Nathan Patin and Eleanor Warnick	7
From the Imitation Game to Techno-Imposters: How AI Became the Ultimate Tool for Psychological Manipulation and Fraud Dr Alexander Stein	11
Part II: Enforcement and Regulation	23
Rethinking Enforcement: The CJEU's H Limited Ruling and its Strategic Value for Creditors in the EU Héctor Sbert, Ph.D.	24
Financial Services Regulator – Force for Good? John Greenfield and David Jones	33
Navigating Regulatory Challenges: Crypto Compliance in the Digital Asset Era Javier Alvarez	39
Panamanian Public Order and its Impact on the Recognition and Enforcement of Foreign Judgments Donald Andersson Saez Samaniego	43

Part III: Asset Recovery Investigations: Criminal, Civil and Technological Perspectives	48
Dealing with the Challenge of Encrypted Messaging Apps Martin Kenney and Harley Thomas	49
Large Language Models ('LLMs') as Translators of Investigative Intuition Kristin Del Rosso	55
Assessing the Suitability of Different Cash Tracing Methodologies Richard Freeman, Marcela Pittelli and Trevor Wiles	59
Asset Recovery in Spain: Civil and Criminal Law Mechanisms Fabio Virzi and Oscar Morales	65
Part IV: Cybercrime	76
Emerging Cyber Security Challenges in Poland Joanna Bogdańska	77
Banks' Liability for Assets Lost in Phishing Schemes Réka Bali and Dóra Kisszabó	85
Ransomware Attacks in Japan 2024 Hiroyuki Kanae and Hidetaka Miyake	90
Recovering Funds from Chinese Onshore Banks for Foreign Telecom-Fraud Victims Andy Liao	95
Scams – Legal Recourse and Protection for Scam Victims in Singapore Danny Ong and Stanley Tan	109

Part V: Tackling Fraud, Corruption and Money Laundering	117
Recovery of Looted State Properties – An Analysis of Ghana’s Latest Asset Recovery Attempt Bobby Banson and Isaac Akyerifi-Mensah Jnr	118
Will the Dam Walls Burst? The State of Play in Turning the Tide on Corruption and Fraud in South Africa John Oxenham, Michael-James Currie and Brandon Cole	134
Corporate Transparency in Anti-Money Laundering: Where are we? Dr Dominic Thomas-James	143
Equitable Liens and Fraud William Fotherby	149
Part VI: Practical Perspectives	156
Should you Agree to Arbitrate in the United States? An Overview and Practical Considerations Joe Wielebinski and Matthias Kleinsasser	157
Recent Developments in U.S. Foreign Sovereign Immunity Jurisprudence Tara Plochocki	168
Asset Investigations in High Net Worth Divorces DC Page	176
Strategic Partners	179

Authors



ISAAC AKYERIFI-MENSAH JNR | Robert Smith Law Group
Isaac.akyerefijnr@gmail.com

Isaac Akyerefi - Mensah Jnr is a Junior Associate in the Labour and Industrial Relations team at Robert Smith Law Group. Having completed his pupillage, he focuses on dispute resolution, with a keen interest in both litigation and arbitration, alongside his work in labour practice. He holds an LL.B. from Central University after which he proceeded to the Ghana School of Law for his BL.

JAVIER ALVAREZ | BDO
jaalvarez@bdo.com



Javier has over two decades of experience providing forensic accounting, litigation support, compliance, expert witness services, and data analytics work, with a focus on digital assets and blockchain. His work includes in-depth investigations of financial fraud, FCPA, risk assessments, due diligence, AML, and regulatory support stemming from BSA/AML/OFAC. He also specializes in asset tracing, specifically the flow of funds within digital assets and traditional fiat currencies. His industry knowledge spans fintech, entertainment, professional and financial services companies. His leadership has been instrumental in several high-profile cases across the US, Latin America, the Middle East, Eastern Europe, Africa, and Southeast Asia. He has a deep understanding of digital asset transactions, markets, and processes, including blockchain technology and decentralized finance protocols. His hands-on experience includes leading blockchain analytics, asset tracing, open-source intelligence, compliance and transaction monitoring tools, which enhance his analytical and forensic capabilities. By leveraging strong collaborations with leading custodians, investment advisors, accounting and tax software providers, he delivers comprehensive, informed solutions tailored to the dynamic digital finance landscape. He advised SEC registrants and privately owned companies on detailed analyses involving asset tracing and reconstruction of complex financial transactions. He has led matters involving financial and securities fraud, embezzlement, Ponzi schemes, circumvention of internal controls, purchase price disputes, misappropriation of corporate assets, bankruptcy matters, and other accounting-related disputes. Javier collaborates closely with external and in-house legal counsel, audit committees, court-appointed receivers, and monitors. He effectively presents findings to regulators, including the SEC, U.S. DOJ, and FinCEN.

RÉKA BALI | Forgó Damjanovic & Partners
balir@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.



BOBBY BANSON | Robert Smith Law Group
bobby@robertsmithlawgroup.com

Bobby Banson is Founding Partner, Robert Smith Law Group, a boutique law firm in the Central Business District of Accra, Ghana. He heads the firm's practice in Alternative Dispute Resolution, Investment Advice and Corporate Governance. He has acted as Counsel in Domestic and International Arbitration matters. He has provided legal services to several multinational Companies doing business across the West African sub region; particularly due diligence of prospective investment opportunities. His wide practice experience includes Corporate, Investment, Real Estate and Dispute Resolution. Educated at Adisadel College, the Kwame Nkrumah University of Science and Technology, and Kumasi-Ghana for his LL.B., he earned his Professional Qualification in Law at the Ghana School of Law, Accra graduating first in the Taxation Law. He holds an LL.M. in International Business Law from the University of Brussels, Certificate in Oil & Gas Contracting, Certificate in Advanced Studies in Arbitration, and Diploma in Financial Management. He has attended courses at Harvard University and the Africa International Legal Awareness (AILA) Conferences. A Fellow of the Chartered Institute of Arbitrators, he has spoken at various conferences organized by CIArb. across the globe and AILA, and participated extensively in SOAS conferences on Arbitration in Africa. He teaches Civil Procedure at the Ghana School of Law. He is author of the book *Civil Litigation in the High Court of Ghana* and several legal articles.

BROOKE BERG | Mintz Group
bberg@mintzgroup.com



Brooke Berg is a Director in the Disputes Practice of Mintz Group where she specializes in complex litigation, and brings her expertise to matters concerning the assets, reputation and personal safety of high-net-worth individuals and their

families. Prior to joining the Mintz Group, Brooke worked to deploy artificial intelligence tools to US government national security agencies for two Silicon Valley startups focused on natural language processing and generation. Brooke spent more than 15 years in the Central Intelligence Agency as an operations officer where she completed five overseas tours, culminating in a tour as a field commander. Brooke speaks fluent Spanish.



JOANNA BOGDAŃSKA | KW Kruk and Partners

Joanna.bogdanska@legalkw.pl

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.

BRANDON COLE | Primerio
b.cole@primerio.international

Brandon is an Associate at Primerio Law, with experience in complex litigation and arbitration across commercial, insolvency, and competition law. He has advised on high-value, cross-border disputes and represented both public and private clients across multiple jurisdictions. Brandon regularly contributes to publications on restructuring, director liability, and regulatory reform.



MICHAEL-JAMES CURRIE | Primerio

m.currie@primerio.international

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.

KRISTIN DEL ROSSO | DevSec
kdr@devsec.com



Kristin Del Rosso is the Cofounder and Managing Director of DevSec. With over a decade of experience in cybersecurity, intelligence, and investigative analysis, she focuses on applying technical expertise to complex cases across financial crime, cyber threats, and national security. With experience spanning hands-on technical research, product development, and broader intelligence analysis, she has worked with corporate, government, and law enforcement stakeholders to support high-stakes investigations. DevSec's mission is to improve the tools and methods for tracking cyber adversaries and analyzing global fraud operations. Beyond her investigative work, Kristin organizes multiple industry conferences focused on intelligence, security, and emerging threats.



NICK DUNNE | Walkers
nick.dunne@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.

WILLIAM FOTHERBY | Meredith Connell
William.fotherby@mc.co.nz



William Fotherby is a Partner at Meredith Connell in New Zealand. He is a trusted advisor to a wide range of public- and private-sector clients. He acts in cases involving suspected fraud and whistleblowing, money laundering and sanctions, contractual disputes, breaches of directors' duties, and employment obligations. He has acted for national governments, financial institutions, large multinational companies, and high-net-worth individuals. William has made hundreds of appearances, at every level of the New Zealand court system. He holds a Master of Laws degree from the University of Cambridge, with first-class honours. He previously worked as an attorney in the London office of an American law firm, in one of the world's best white-collar-crime practices. In 2017, William was admitted to the English Bar and is a member of Middle Temple. In 2023, he was admitted to the bar of the Pitcairn Islands. He is a former editor-in-chief of the Auckland University Law Review.



RICHARD FREEMAN | FRA
rffreeman@forensicrisk.com

Richard Freeman is a Director in FRA's London office. He is a forensic accountant with over 15 years' experience in matters involving fraud and corruption, internal investigations, regulatory investigations, and due diligence. His experience spans a wide range of industries, including banking, oil and gas, manufacturing, and pharmaceuticals. Richard regularly works with clients and their external counsel on investigations. He has recently managed investigations related to revenue recognition, related party transactions, asset misappropriation, potential sanctions breaches, and allegations of non-financial misconduct. Richard also has experience working on disputes that require tracing transactions banking and financial information to determine their beneficiaries.

JOHN GREENFIELD | Mourant
John.Greenfield@mourant.com



John undertakes the complete range of major litigation and advocacy work including asset tracing, multi-jurisdictional disputes and commercial and trust litigation. John has been Counsel in many of the major litigation cases before the Royal Court of Guernsey and the Guernsey Court of Appeal and is one of the few Guernsey advocates to have appeared as counsel in the Privy

Council. He has been lead counsel in ground-breaking trust litigation cases in the past 12 months. John was a founder member of the Guernsey Royal Court Working Party which completely reviewed the island's Civil Procedure in 2008 and is a member of the UK Fraud Advisory Panel. He is a founder member of ICC FraudNet. He is also a member of the Association of Contentious Trust and Probate Specialists and is a Notary Public. John was the first elected Head of the Guernsey Bar in November 2008 and was re-elected to the role in 2010. In 2014 John was awarded ACTAPS Offshore Contentious Lawyer of the Year Award. In 2015 he was awarded the "most highly regarded" classification for Asset Recovery by Who's Who Legal – one of only five offshore lawyers in the world to be awarded such accreditation.



DAVID JONES | Carey Olsen

david.jones@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 multijurisdictional 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).

HIROYUKI KANAE | Anderson Mori & Tomotsune

hiroyuki.kanae@amt-law.com



Hiroyuki Kanae focuses on corporate law, including mergers and acquisitions (domestic and international), corporate reorganizations, joint ventures, labor and employment law (including dispute settlements), corporate governance, IP license agreements, and real estate transactions. He also advises on commercial litigation matters, including domestic and cross-border litigations involving major Japanese and foreign companies. He represents major Japanese manufacturing companies, foreign financial institutions and high tech companies, as well as private equity funds. He has been advising on the global development projects mainly for the major Japanese companies investing in North America, Europe and Asia pacific regions and has more than

30 year experiences in the cross-border M&A. In recent years, he has completed M&As and joint ventures not only in Europe and the North America but also in Asian and pacific rim developing countries by collaborating with rich overseas networks in the areas of semi-conductor, high tech, nano-tech, aviation and space, pharmaceutical, medical equipment and software industries. Through experience of a member of the audit and supervisory board of a major logistic company that has been seeking the global strategy, he advises on the real need of management strategy foreseeing the post-merger integration.



MARTIN KENNEY | MKS LAW

mkenney@mks.law

Martin Kenney is one of the world's leading asset recovery lawyers, specialising in multi-jurisdictional economic crime and international serious fraud. He has acted for international banks, insurance companies, individual investors, and other private and governmental institutions. Based in the British Virgin Islands, Martin is founder and Head of Firm at MKS Law (previously Martin Kenney & Co). The firm's work lies at the intersection of cross-border insolvency, creditors' rights and complex commercial litigation: WIRED styled the firm as among "the world's sharpest fraudbusters". Leading a team of lawyers, investigators and forensic accountants, Martin is widely regarded as a ground-breaker in the use of pre-emptive remedies, multi-disciplinary teams and professional litigation funding in response to global economic crime, uprooting bank secrets and freezing hidden assets in multiple jurisdictions. He is a practicing solicitor advocate of the senior courts of England and Wales, the Eastern Caribbean at the BVI, at St Vincent and the Grenadines, and a licensed foreign legal consultant in the state of New York. Martin is also a Visiting Professor at the University of Central Lancashire (UCLan) School of Law and Policing in the UK, and ranked among the world's leading asset recovery lawyers by Chambers and Partners as well as being a Lexology Index "Global Elite" Thought Leader.



DÓRA KISSZABÓ | Forgó, Damjanovic and Partners

kisszabod@fdlaw.hu

Dóra Kisszabó is an associate at Forgó, Damjanovic and Partners Law Firm. She works in several different practice areas including dispute resolution and claim enforcement, regulatory compliance, commercial law, employment law and IT-IP cases. Holding an LL.M. degree in data protection and cybersecurity law, she possesses a deep understanding of the risks of privacy infringement in both a business and personal context.

MATTHIAS KLEINSASSER | Winstead

mkleinsasser@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.



RONGHUA (ANDY) LIAO | Han Kun Law Offices

Andy.liao@hankunlaw.com

Andy is a partner at Han Kun Law Offices dispute resolution department, specialising in litigation and arbitration, fraud, asset tracing and recovery, foreign judgment and award enforcement as well as white collar & financial crime. In terms of international fraud, Andy is one of the few PRC lawyers widely recognized by the international legal community. Over the years, he has represented Han Kun Law Offices to author the China chapters for several international publications in the area of fraud and asset recovery, including the Asset Tracing and Recovery Review, Chambers Global Practice Guides - International Fraud & Asset Tracing as well as the CDR Essential Intelligence: Fraud, Asset Tracing & Recovery, where Han Kun is the only law firm from China. Andy has enormous knowledge and in-depth understanding in his specialised areas, and has represented a number of banks, companies and HNWIs from various jurisdictions and successfully traced and recovered their defrauded funds. Based on his distinguished performance in dispute resolution, Andy has been rated by The Legal 500 as a highly recommended dispute resolution lawyer in the Asia Pacific for 2019 and 2021. Andy is an arbitrator of Shanghai International Arbitration Centre.

HIDETAKA MIYAKE | Anderson Mori & Tomotsune
hidetaka.miyake@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.



OSCAR MORALES PH.D. | Cases & Lacambra
oscar.morales@caseslacambra.com

Oscar Morales is a partner at Cases & Lacambra. He leads the White Collar, Internal Investigations and Regulatory Enforcement practice. Oscar is Ph.D. in Law, he is currently a lecturer at the Ramón Llull University (ESADE) and has been a lecturer in various Spanish and foreign Universities. He has over 30 years' experience in investigation and teaching. He is the author of several books and academic articles on financial crimes, bribery corruption, securities fraud and crimes against labour rights. He is a regular lecturer and has organised seminars and training courses for judges in the Spanish General Council of the Judiciary. He has been a partner at one of Spain's leading law firms over thirteen years. Oscar has an extensive experience in preventive legal advice to corporations and management, designing and implementing crime prevention models for corporates and developing a wide range of internal investigations. He has defended the interest of various financial and banking institutions and of the members of their executive management, financial directors and, in some cases, members of the Board of Directors in complex matters. He has also represented multinational companies of various sectors of activity, such as energy, fashion and luxury, consumer goods, health, and infrastructures, before professional and jury courts. Oscar Morales was a magistrate at the Barcelona Provincial Court for four years. He has been regularly recognised by the most important legal Directories, such as Chambers & Partners as one of the leading practitioners in white collar in Spain.

DANNY ONG | Setia Law
danny.ong@setialaw.com



Danny Ong is Managing Director of Setia Law and specialises in complex international commercial and financial disputes and investigations, as well as cross-border restructuring and insolvency. Danny has led multiple high-stakes cross-border disputes and investigations, across a multitude of industries over the last two decades. He is regularly called upon by financial institutions, private investment funds, and state-owned enterprises, to act in mandates involving complex investments, market misconduct, and distressed situations. He is also known for his expertise in international enforcement, fraud, and financial crime and is recognised amongst the Global Elite as one of 40 Global Thought Leaders in the asset recovery field. With extensive experience in multi-jurisdictional headline restructurings and insolvencies, Danny is recognised as a “standout” in the market. His portfolio includes acting for debtors in the Eagle Hospitality REIT restructuring, and acting for the liquidators of 45 Lehman entities across Asia (ex-Japan), MF Global Singapore, Dynamic Oil Trading (of the OW Bunker Group), and BSI Bank. More recently, Danny has been a pioneer in disputes and managing crises in the blockchain and digital assets space, having led the team that successfully prosecuted the first cryptocurrency claim before the Singapore International Commercial Court, and advising distressed cryptocurrency investment platforms. Danny combines technical excellence with sharp commercial sensibility and creativity in tackling novel legal questions. He is spoken of by clients as “an excellent litigator” and “an outstanding lawyer” who is “adept at tackling unique and challenging issues” and “combining a deep and broad knowledge of the law with a pleasant manner and an ability to switch gears and become a powerful advocate and highly effective cross-examiner”. Danny graduated from the National University of Singapore and is admitted to the Singapore Bar as well as the Rolls of Solicitors of the High Courts of Hong Kong and England and Wales.



JOHN OXENHAM | Primerio
j.oxenham@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.

DC PAGE | V2 Global
dcpage@v2-global.com

As the Managing Partner of *V2 Global*, DC directs worldwide operations. His experience spans a career including US Customs (Homeland Security), Kroll Associates and CEO of Verasys. His focus includes multi-jurisdictional inquiries involving asset tracing, litigation support, anti-money laundering and investigations for multi-national corporations. With his customs background, DC and his team have assisted many multi-nationals and sovereigns with asset tracking and recovery investigations. Complex cross-border inquiries require the integration of multi-dimensional investigators capable of private-public sector liaison. DC has perfected and replicated such inquiries around the world creating value for corporations and at the same time, results for governments.



NATHAN PATIN | Mintz Group
npatin@mintzgroup.com

Nathan Patin is a director based in Denver, Colorado and head of the firm's Digital Investigations practice. He leads the Digital Investigations Group (DIG), a company-wide team of more than a dozen investigators at the cutting edge of online investigations. DIG's diverse team ranges from former data and investigative journalists to federal agents and seasoned online researchers, all of whom bring deep expertise in uncovering hidden information on the internet. Since joining the Mintz Group in 2016, Nathan has worked on hundreds of investigations, including matters involving asset tracing; cryptocurrency; intellectual property theft; and hack-and-leak campaigns. Nathan has been a member of award-winning investigative collective Bellingcat since 2015 and has provided digital investigations training for dozens of journalists, researchers and investigators around the world. He has been interviewed or cited by The New York Times, National Public Radio, CNN International, the Associated Press and other major media outlets. He has also presented his research at prominent conferences, including CYBERWARCON. Nathan served as an adjunct professor at Georgetown University, where he created and taught the Hands-On Open-Source Investigation (SEST-656) course for master's students in the Security Studies Program.

MARCELA PITTELLI | FRA
mpittelli@forensicrisk.com



Marcela is an Associate Director in FRA's Paris office. Her expertise includes law enforcement monitorships, internal fraud and anti-corruption investigations ("ABAC"), fine and disgorgement calculations, OFAC sanctions, and M&A/programmatic due diligence. Marcela's representative investigative experience includes: FCPA monitorships both on the monitor's and company's sides; disgorgement calculation for an energy infrastructure services provider; post-acquisition FCPA compliance reviews for global providers in the hospitality and insurance brokerage industries; review of the third-party screening and due diligence monitoring process for a global oil company; compliance assessments for a major technology and software infrastructure company's third parties in Latin American jurisdictions, including Brazil, Colombia and Mexico; and an internal fraud investigation for a multinational chemical company.



TARA J. PLOCHOCKI | Sequor Law
tplochocki@sequorlaw.com

Tara Plochocki's legal career is marked by a commitment to justice, international collaboration, and the strategic resolution of complex legal challenges. She litigates a wide range of transnational claims arising from breaches of contract, racketeering, fraud, defamation, and tortious business practices, both at the trial and appellate levels. Tara obtains recognition of foreign arbitral awards and judgments to facilitate asset recovery efforts. Her expertise extends to conducting post-judgment discovery and initiating discovery actions under 28 U.S.C. § 1782 to gather evidence for use in foreign proceedings. Tara also advises international clients on treaty application and interpretation, jurisdictional matters, and US litigation strategies. Tara is the first Washington D.C.-based attorney for Sequor Law, establishing the firm's presence in the nation's capital, and is the Washington, D.C. member of ICC Fraudnet. In addition to her international civil litigation practice, Tara represents individuals in connection with congressional and law enforcement investigations. She also advises on extradition law and regularly serves as an expert in proceedings in the UK and other Commonwealth countries. Tara regularly speaks at global conferences on fraud and asset tracing, as well as the extraterritorial application of U.S. law. Tara is dedicated to pro bono service and litigates matters at the intersection of constitutional rights, international law, and national security. She successfully represented detainees in Guantanamo Bay when she won the first habeas petition in over ten years, construing the laws of war to obtain the release of her client. She also challenged the U.S.' designation of individuals for death by drone strike,

including obtaining a ruling that U.S. citizens have a constitutional right to due process before they may be targeted by the US. Tara also authors amicus briefs on behalf of individuals and organizations on issues of fairness in education, criminal justice and national security.

DONALD ANDERSSON SÁEZ SAMANIEGO | MDU Legal
dsaez.mdu@gmail.com



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 crossborder); 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.



HÉCTOR SBERT, Ph.D. | ECIJA
hsbert@ecija.com

Héctor is a partner in the litigation and arbitration, restructuring and insolvency and compliance areas of ECIJA's Barcelona office. He has more than 20 years of experience advising national and international clients from all sectors in the areas of litigation, arbitration and insolvency law. He has been recognized by prestigious rankings such as "Best Lawyers" and "Who's Who Legal" among the best lawyers in Spain in his areas of practice. He is also a specialist in litigation linked to cryptocurrencies, cybersecurity and cyber fraud, as well as fraud related to unconventional assets, such as wine products and art and collectibles. He is the representative for Spain of ICC FraudNet and a Member of the Chartered Institute of Arbitrators of London (MCIArb.) and a Registered Mediator with the Ministry of Justice. Héctor holds a PhD in Law from the Universitat Pompeu Fabra, an Executive MBA from IESE, and a law degree from the Universitat Pompeu Fabra. In addition, he has been a member of the Governing Board of the ICAB (Barcelona Bar Association) and has chaired the Bar Association's Ethics Committee. Héctor speaks Spanish, Catalan, English, French, German and Italian.

DR ALEXANDER STEIN | Dolus Advisors
alexanderstein@dolusadvisors.com



Alexander Stein is founder and managing principal of Dolus Advisors, a strategic consultancy that advises senior leaders and boards of directors in issues involving leadership, culture, governance, succession, and other institutional matters with complex psychological underpinnings. Trained and licensed as a clinical psychoanalyst, Dr Stein leverages deep expertise in human decision-making, behavior, and the influences of power and psycho-social dynamics in organizational ecosystems to help executives understand and address enterprise challenges. An internationally regarded authority in the psychodynamics of fraud and abuses of power, Dr Stein is frequently engaged in multijurisdictional serious fraud and corruption matters. Dolus' other practice areas include psychologically incisive leadership assessment and development, and architecting and leading CEO succession and transition processes; elevating board effectiveness and governance capabilities; developing and implementing psycho-socially sophisticated programs concerning cybersecurity, human risk, and corporate culture and ethics; and assisting technology innovators and investors to ensure frontier agentic computational systems are ethically and socially aligned with human needs. He is a Specialist Collaborator in the Center for Human Centered Cybersecurity (HCC) of The National Institute of Standards and Technology (NIST), and sits on several advisory boards, notably including PsiAN, a leading mental health advocacy organization. Dr Stein is widely published and cited and a former contributor to Forbes, Fortune, CNN, and CBS Business News. He is currently the Editor-in-Chief of The CAI Report, a publication of the American Psychoanalytic Association delivering insights and commentary at the intersection of psychoanalysis and artificial intelligence. He is a frequent podcast and webinar guest, on-camera commentator, and keynote speaker and panelist at conferences, symposia, and corporate events internationally.



STANLEY TAN | Setia Law
stanley.tan@setialaw.com

Stanley Tan is an Associate at Setia Law. Stanley has acted in a broad range of cross-border disputes and investigations where he specialises in the prosecution of claims involving multi-jurisdictional fraud, and the tracing and recovery of digital assets. His experience and familiarity with cryptocurrency and emerging technologies often sees him working together with experts and industry leaders on complex briefs and dealing with novel issues of law. Stanley aspires to develop a specialist advocacy practice that focuses on digital technology, Web 3.0, and disputes in cyberspace. Stanley graduated from the National University of Singapore with First Class Honours. He was awarded the Outstanding Undergraduate Researcher Prize for his research relating to the loss or

destruction of evidence. He was also placed on the Directors' List while studying at the Centre for Transnational Legal Studies in London. He represented his university in the Willem C Vis International Commercial Arbitration Moot (Vienna), and was also a finalist in the Dentons Rodyk Moots and a semi-finalist in the Advocacy Cup.

HARLEY THOMAS | MSK LAW

hthomas@mks.law



Harley Thomas is a forensic accountant and senior investigator, a core part of our investigations team.

He joined MKS Law in July 2022, after completing a Master's degree in Financial Investigation at the School of Law and Policing at the University of Central Lancashire (UCLan), achieving a Distinction. Prior to this, Harley graduated with a First-Class degree in Accounting and Finance, also at UCLan, and was recognised in the Dean's List awards for both degrees.

Harley is a full practicing member of the ACCA (the Association of Chartered Certified Accountants), having become a Chartered Certified Accountant in 2021. He is also a Certified Anti-Money Laundering Specialist (CAMS) with the Association of Certified Anti-Money Laundering Specialists (ACAMS), and a Certified Fraud Examiner (CFE) with the Association of Certified Fraud Examiners (ACFE). He trained with a local firm in Blackpool, England, starting as an accountant in 2017, then moved to KPMG as Audit Assistant Manager in 2021, managing audit engagement for a range of clients, including FTSE-listed entities. He has wide-ranging experience in audit and assurance engagements, corporate accounts, corporate taxation, business and personal tax, along with other finance and accounting-related matters.



DR DOMINIC THOMAS-JAMES | ICC FraudNet

dominicthomasjames@cantab.net

Dr Dominic Thomas-James is Consultant, Director of Publications and Editor of the Global Annual Report on Fraud and Asset Recovery for ICC FraudNet. He is a Global Justice Fellow at Yale University, and teaches at the University of Cambridge. Dr Thomas-James is a Barrister at Goldsmith Chambers, London and was called to the Bar of England and Wales by the Inner Temple. He is a qualified civil and commercial mediator accredited by the ADR Group. He has consulted to various intergovernmental and international organisations, and is a Senior Organiser of the annual Cambridge International Symposium on Economic Crime at Jesus College, Cambridge. Dr Thomas-James earned his Ph.D., and M.Phil., from Queens' College, Cambridge and his LL.B., from King's College London. He is author of the book *Offshore Financial*

Centres and the Law: Suspect Wealth in British Overseas Territories (2021, Routledge) and numerous other book chapters, edited texts and journal articles.

FABIO VIRZI | ECIJA
fvirzi@ecija.com



Fabio Virzi is a partner at ECIJA in the litigation and arbitration team. He has extensive experience advising all kind of clients in the resolution of civil and commercial disputes, both in the pre-litigation phase and during the proceedings. He specializes in civil and commercial litigation before the Spanish Courts and has an extensive experience in matters relating to obligations and contracts, noncontractual liability, corporate affairs, unfair competition, directors' liability, shareholders disputes, amongst others. Furthermore, Fabio has a strong track record in the enforcement of national and foreign judgments and awards, as well as in asset tracing and recovery. Fabio is an expert on litigation relating to the finance, banking, construction, and insurance industries sectors, as well as to M&A transactions and private equity. Fabio is also an expert in the field of domestic and international arbitration. He has taken part in domestic arbitration proceedings before the leading Spanish courts of arbitration (the Civil and Commercial Court of Arbitration and the Madrid Court of Arbitration, etc.), as well as in international arbitrations under the rules of the International Chamber of Commerce (ICC).



ELEANOR WARNICK | Mintz Group
ewarnick@mintzgroup.com

Eleanor Warnick is a managing investigator at the Mintz Group, where she specialises in cross-border asset tracing, litigation support and fraud detection. She has eight years' experience in investigations, including five years in corporate intelligence and three as a journalist. During this time, she has advised a broad range of clients such as financial institutions, law firms, government bodies and multilateral institutions. Recent casework includes: unearthing procurement fraud at a political organisation; exposing grand corruption under a former government of an African nation; and uncovering an extortion attempt at a logistics company in Guatemala. Prior to joining the industry, she was a journalist, editor and commentator, focusing on Latin American current affairs. During that time, she undertook on the ground investigative assignments and carried out hundreds of interviews in countries such as Bolivia, Brazil, Mexico and Peru. She holds a BA in Spanish and Portuguese from Oxford University, is a

Certified Fraud Examiner (CFE) and a Certified Cryptocurrency Investigator (CCI).

JOE WIELEBINSKI

joewielebinski@gmail.com



After 40 years of practice, Joe recently retired from the practice of law but remains active in a variety of legal matters. 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.



TREVOR WILES | FRA

twiles@forensicrisk.com

Trevor Wiles is a Partner in FRA's London Office in the Forensic Accounting team. He has more than 30 years of experience in forensic services focusing on helping clients and their legal advisors navigate complex and multi-jurisdictional matters resulting from whistleblower and or regulator actions. Trevor specializes in helping clients respond to serious misconduct allegations, including bribery and corruption, accounting misstatement, money laundering, embezzlement, procurement fraud, sanction breaches, channel stuffing, and asset misappropriation. He has supported clients with disgorgement and fine calculation analysis with regard to settlements with prosecuting authorities. Most recently, he supported Entain plc in relation to an HM Revenue & Customs investigation, resulting in the first ever Deferred Prosecution Agreement with the UK Crown Prosecution Service and a GBP 585m settlement.

ICC FraudNet
Global Annual Report 2025

Part I: Current Perspectives on Artificial Intelligence

iccfraudnet.org



ICC FraudNet
Global Annual Report 2025

Breaking the Iron Triangle? The Future of AI Decision Making in Litigation

NICK DUNNE



Breaking the Iron Triangle? The Future of AI Decision-Making in Litigation

Nick Dunne
Walkers (Cayman) LLP

Abstract

Against the background of a seemingly exponential growth in the use of AI in society, this article takes a brief look at some of the key issues that should be taken into account when considering the expansion of its role within the litigation system, particularly where fraud cases are in issue.

Introduction

"*Cheap, Quick, Good- pick any two*" - the "Iron Triangle" is a familiar dilemma for decision makers. It is equally well-known to fraud lawyers, where the management of scarce resources in pursuit of a positive outcome is a recurring theme in litigation.

AI only entered the wider public consciousness with the release of ChatGPT in late 2022, but less than 3 years later it has percolated throughout society, from shopping, to mobile telephones, to refrigerators. And whilst it is easy to laugh (or cringe) at stories of lawyers caught out relying on fictional AI generated cases, tools such as technology assisted document review are a well-established part of the litigation landscape.

For lawyers, the question has therefore evolved from "*should we?*" into "*could we?*". There are intriguing possibilities: might AI be deployed not only as a counter to the documentary blizzard, but also to determine cases? The touted rewards are tempting and, on their face, have the capability to shatter the Iron Triangle, simultaneously

offering less delay, reductions in costs, and greater consistency. That cannot be lightly dismissed, least of all in fraud cases where delay, complication, and obfuscation are common features of wrongdoer strategy.

This article does not presume to evaluate the legal capabilities of AI, but in a world where GPT 3.5 failed the bar exam in the bottom 10th percentile, whereas barely a year later GPT 4 passed it in approximately the 90th percentile, it would be naïve to assume that performance will not continue to improve at a significant rate. Rather, it briefly examines three of the less tangible features of the legal process and the extent to which they can be reconciled with an enhanced role for AI.

Transparency

From infancy, we are taught to show our working: it is not simply a matter of issuing a "correct" answer, but one which is provably so. By the same token, it is not sufficient for a judicial process to merely designate one side the winner, and the other the loser: an effective system must display its reasoning so parties can evaluate (and challenge) the judge's thought process.

At first glance, AI might appear capable of effectively simulating that process: it can plainly produce written decisions with support. However, what cannot be derived from that written output is an understanding of the underlying engineering that drives its generation. How has the model been programmed? By whom? What has it learned? And what is the process for applying that learning?

It might fairly be said that the same opacity exists in the case of a human decision maker; after all, it is almost impossible to truly know the mind of another, and the experiences and personal characteristics that might feed into a judicial decision will rarely be apparent to the subjects of that decision. However, the human decision maker benefits from an inherent measure of trust that we are rarely willing to place in a machine, in the same way as many of us might feel more comfortable being driven by a taxi driver, even one we have never met before, than we would do being carried in an automated self-driving car.

That trust, or lack of it, feeds into what might broadly be termed "customer satisfaction". Judicial decisions only attract respect where the participants are confident in the integrity of the process through which they have been made, and it seems unlikely that will ever be true of a wholly technology-based process: simply being told to "trust the algorithm" is not enough. In a world where institutions such as banks and governments have increasingly sought to achieve savings through automation, the universal reaction to an adverse experience is to try and "talk to a human" in the hope that common sense will prevail. There seems little reason to believe that any greater level of trust would be inspired by AI based decision making.

Evolution

One of the great strengths of the common law has been its capacity for development to meet changes in the world. Not much more than fifty years ago lawyers had not encountered the Mareva injunction, or the Norwich Pharmacal order, yet now they form core elements of asset recovery practice.

Those developments are wholly a product of judicial initiative. Evolution of the common law is achieved not by turning over the right stone to discover something already in existence but hitherto hidden, but instead by judges reacting to new situations, or societal change, by redrawing the map.

It is important to consider whether AI decision making could coherently move beyond the application of existing law, into the more nuanced task of adapting the law to fit changing circumstances. A dogmatic approach based only on what can be learned from the past runs a clear risk of losing sensitivity to novel situations.

For all the current enthusiasm to criticise judicial "activism", flexibility is a key part of a functioning and modern system at all stages of the process: if anything, interlocutory applications can call for an adaptable approach more often than might be the case at trial. That cannot be effectively addressed only by the provision of a human "safety net" by way of appeal – unless flexibility is available at the critical moment in time, it loses much of its usefulness.

Biases

Perhaps more difficult to evaluate is the potential of AI to reduce bias. Although the common law system traditionally places significant reliance upon the ability of decision makers to determine credibility, a significant body of research suggests that humans, regardless of training, are signally poor at that assessment, often relying upon prejudices about what someone telling the truth should look like and getting it right no more often as they get it wrong. Against that background, a technologically based decision maker who is not conscious of, let alone reliant upon, verbal or physical prompts, might seem to offer a focus on substance over style.

However, at their best, court hearings should be a two-way process, getting to the heart of a matter not only by providing each party with an opportunity to put what they feel is their best case, but also to address the points that the decision maker considers to be particularly important. That communication is an inherently human process, and although there is always a risk of trespassing into performance, it is difficult to imagine that exchange taking place in any meaningful way between human and computer.

Furthermore, law is a societal construct, society is comprised of people, and on some level, every case is about people. Many lawyers would point to a "feel" for cases being a feature of the best judges, an ability to manage and decide a case whilst accounting

for the personalities involved, whether on the part of parties, witnesses or lawyers. Whilst "feel" could be dismissed as a synonym for internal biases, it can also quite reasonably be seen as a necessarily human element in applying rules created by humans. If we view law as a product of human creativity and endeavour and not observed scientific fact, the case for saying that it should be applied in a scientific or mechanical way is greatly weakened.

It may be that matters circle back to the "customer satisfaction" mentioned above. In seeking their day in court, parties look for the opportunity to explain their case to a judge in the most persuasive way that they can, not to throw themselves on the mercies of an algorithm. The imprecision and foibles of human judgment may be a necessary cost of maintaining a system which meets our sense of what is just.

A Brave New World?

There is of course a risk of becoming a Luddite. The world changes rapidly, and just as the farmers of the 19th century and children of the late 20th century rapidly became comfortable with technologies which were inconceivable to their parents, let alone grandparents, so it seems reasonable to assume that the same will be true of the children of the early 21st century: increased familiarity may ultimately be sufficient to create the necessary level of confidence to move towards a greater role for AI decision making.

For now, however, a measure of caution is justified. The Iron Triangle may well have been significantly weakened, with speed and accuracy now achievable in some tasks without incurring material (or indeed any) increase in cost or team size, which can in turn level the playing field, limiting the litigation advantage that hitherto has often accompanied a greater access to resources. If legal spend becomes less of a tactical trump card, that is undoubtedly good news for the asset recovery lawyer facing a fraudster well-resourced with other people's money.

That is, however, light years from entrusting the actual resolution of cases, or even interlocutory applications, to technology. A core principle of asset recovery must be doing justice, and if innovation is pursued without a secure foundation of public confidence, that justice may prove elusive.

ICC FraudNet
Global Annual Report 2025

Staying a Step Ahead of Fraudsters in the Age of AI

**BROOKE BERG, NATHAN PATIN
AND ELEANOR WARNICK**

iccfraudnet.org





Staying a Step Ahead of Fraudsters in the Age of AI

Brooke Berg, Nathan Patin & Eleanor Warnick
Mintz Group

Introduction

If AI is revolutionising banking, finance and commerce, it is having the same dramatic effect in the underworld, giving bad actors powerful new capabilities and amplifying the harm they can inflict. For example, AI is enabling fraudsters to create convincing emails that appear to be from banks or payroll departments for use in phishing attacks. Fraudsters are also using AI-powered voice cloning to impersonate executives, bank representatives or even family members in real-time phone scams, tricking victims into transferring money or disclosing sensitive information. AI's ability to automate transactions and quickly generate legitimate-seeming invoices and contracts makes money laundering harder to detect. Investment scams are made more convincing through deep faked news articles and celebrity endorsement videos.

Perhaps most importantly, AI-driven fraud makes it easy for bad actors to cast a wider net, significantly expanding the pool of organisations and individuals at risk of becoming threat targets. Phishing scams, for example, are no longer labour-intensive; AI can now generate and personalise them at scale. As a consequence, rather than focusing on large organisations—which generally can be counted on to have sophisticated defences—bad actors can now profitably target a large number of smaller, and possibly more vulnerable, entities.

Looking beyond an AI Arms Race

Naturally, investigators and others charged with risk mitigation, fraud detection and asset recovery have responded in kind, developing AI-driven tools and approaches to monitor threats and ferret out malfeasance. But the new threat landscape requires more than keeping up in a technological arms race. When AI has given fraudsters the ability to move quickly, obfuscate with mounds of data and to generate fake identities, investigators must double down on three traditional imperatives: speed and accuracy, differentiating signal from noise, and identification and disambiguation. While these capabilities have always been important, they are now the central pillars of investigative work, and the processes used by investigators must evolve accordingly.

For example, a large category of investigative work involves combing through troves of data to extract patterns, as when a case requires slogging through thousands of dense Security Exchange Commission (SEC) filings in an effort to identify a subject's holdings for asset recovery. Historically, this has required a brute-force approach, constructing elaborate spreadsheets to map transactions or connections between entities. Now, however, AI-powered tools that have been appropriately trained can conduct such analysis almost instantaneously, not just mapping holdings and fund flows, but uncovering ultimate beneficial ownership.

AI also makes it possible to identify patterns in much larger datasets, such as those generated by social media. Recently, for example, we were asked to help identify the distributors of counterfeit Covid home testing kits. We realised that social media posts about the product created a map of the product's end users; we were able to use an AI-powered tool to reverse-engineer the distribution chain to help point to the source of the counterfeit goods.

AI-powered social media analysis is also useful when high-profile disputes play themselves out online. In such conflicts, it is important to know how much of the venom is the organic by-product of vocal supporters taking sides and how much might be due to a smear campaign orchestrated by the opposition. Hours of podcasts and YouTube videos can be automatically transcribed and analysed for tell-tale clues; other tools can then analyse those transcripts and social network traffic to identify key influencers, who can then be scrutinised to see if they are linked to troll farms. Similarly, AI tools can be used to see if online attacks on brands are being initiated by competitors or other economically motivated actors, or to help distinguish genuine threats from background chatter in cases of ongoing online harassment.

In addition to accelerating the investigative process and separating signal from noise, AI tools are also enabling investigators to enhance identification and disambiguation. In one recent case, we were asked by the administrator of a professional credentialing exam to help crack an online cheating ring operating on a Discord server. While the ring members all used aliases, we were able to link one member to an anonymised online account in which he had posted a photo of himself—but in which his face was

pixelated. But just as AI tools can create fake images, it can also unscramble digitally altered photos. While we couldn't do so perfectly, it was enough to allow a second AI platform to help us identify the subject in the photo.

New Possibilities Demand New Approaches

These case studies illustrate the range of ways in which AI can be harnessed to make investigations faster and more effective. But these examples also highlight important principles underlying the use of AI. First, while AI provided the critical capabilities in each of these cases, AI is only a tool that is as effective as the investigators using it. AI platforms thus operate best when they are essentially virtual members of an experienced investigative team: AI-generated insights provide a foundation that investigators then refine through experience, intuition and contextual knowledge. The effective use of AI thus depends on its effective integration into the investigative workflow.

Second, cutting-edge application of AI requires investigators and others on the front lines to think more broadly about data and information. Using AI to extract information about named entities in piles of SEC reports is a fairly straightforward use case. But to use AI to construct influencer networks from social media data, it helps to have a basic understanding of network structure. To be sure, as new uses of AI become standard practice, it will be less necessary to grasp the theoretical underpinnings of various AI use cases. But broader awareness allows one to be at the forefront of what is possible.

Finally, investigations firms need to adopt a stance of constant evolution with respect to AI. In some ways, investigations and AI are now in a position similar to that of the internet and the publishing industry at the beginning of this century—the technology is moving from the periphery to the centre and gaining speed in doing so. The disruptions of the internet forced publishers to not just re-centre their product and its distribution, but to reimagine what was possible. Similarly, in the face of the rapid evolution of AI, investigators are having to evolve their processes and workflow to match a new vision of what it means to extract true knowledge from mere data.

The emergence of AI has irrevocably altered the landscape for both fraudsters and those who pursue them. The same technological advances will be available to both sides. The advantage, then, is likely to lie with whomever can best adapt to the changes that AI brings.



ICC FraudNet
Global Annual Report 2025

From the Imitation Game to Techno- Imposters: How AI Became the Ultimate Tool for Psychological Manipulation and Fraud

DR ALEXANDER STEIN



From the Imitation Game to Techno- Imposters: How AI Became the Ultimate Tool for Psychological Manipulation and Fraud

Dr Alexander Stein
Dolus Advisors

Abstract

Today's advanced technologies are ushering increasingly more complex forms of fraud and economic crime unleashed at previously unimagined velocity and scale. Frontier AI systems in particular represent an unprecedented convergence of technology and psychology. Machine agents are designed to operate autonomously in society in ways indistinguishable to humans and eradicate a conscious sense of interacting with a non-human entity. No longer merely a cutting-edge instrument in the knowing commission of nefarious activities, agentic AI can now itself function as an imposter – the assumption of a false or disguised identity to deliberately deceive. We are entering uncharted territory where the fraudster is not a person but a computational system. Techno-imposturousness isn't equivalent to a Trojan horse, a boiler room, Nigerian prince, or charlatan's grift. We are being groomed to willingly enable what may come to be understood as the most far-reaching and consequential fraud in history – blindly abdicating human agency to computational fakery.

"People will come to adore the technologies that undo their capacity to think."

– Aldous Huxley

People have been swindling one another for thousands of years. In 300 BC, in what is acknowledged as the earliest recorded case of fraud, Hegestratos and Zenosthemis, two Greek sea merchants, attempted to perpetrate a maritime insurance scam by trying to pocket the proceeds of a loan advanced on an insurance policy covering their ship and its cargo.

While the types and techniques of fraud have evolved over the centuries, its psychological underpinnings remain unchanged. Fraud, as I have long maintained, is a crime of relationships, predicated in universal human propensities to be hoodwinked and manipulated. Trust cannot be broken unless it is first given.¹ One party willfully disadvantaging another through deception, betrayals of trust, or abuses of power is, irrespective of tangible losses or other material harms, intrinsically and dominantly psychological.

Understanding that each of us can be duped or gas-lit into thinking, believing, or feeling anything, is a driving principle in all forms of malevolent creativity – producing innovative or novel solutions with the express intent of harming others rather than for socially constructive purposes. It follows that the lengths people will go to deceive, manipulate, or betray others’ trust has no bounds.

Not surprisingly, advances in technology opened new vistas of opportunity for wrongdoers and brought increasingly more complex forms of fraud unleashed at previously unimagined velocity and scale. Misconduct that once required meticulous labor to execute – physical impersonation, for instance, or the hand-crafted forgery of financial instruments, documents, and signatures – evolved, beginning in the late 1980s, to replicating and skimming credit cards with a keystroke. The rapid expansion of the internet in the 1990s as a publicly accessible global network further enabled bad actors to commit identity theft, phishing scams, and many other sophisticated online fraud schemes through easy access to vast pools of information and the ability to target countless numbers of victims with minimal effort.

Today, advanced and emerging technologies, particularly the mass proliferation of social media and the advent of AI systems, chatbots, and automated agents deployed in propaganda and mis- and disinformation campaigns, are fueling rampant, ascendant fraud and corruption. The sheer compute power and capacity for hyper-scaling has already overwhelmed conventional bulwarks against economic crime, cyber warfare, geo-political destabilization, and other wrong-doing.

There is a substantial and still-growing body of evidence demonstrating how AI is already impacting contemporary life: algorithmic bias, wide-scale disinformation and social manipulation, the pillage of privacy, the weaponization and profiteering of

¹ Stein, Alexander. *Innovations and Strategic Applications in the Psychology of Fraud*, 2023 ICC FraudNet Global Report — Fraud and Asset Recovery in an Unstable World

personal data, intrusive apartheid-esque surveillance, impingements on cognitive liberty, deep fakes and the erosion of verifiable objectivity created by a deluge of synthetic slop and plausibly credible but actually incorrect data. There are a plethora of computational applications and services designed to monitor, assess, surveil, predict, manage, influence, and manipulate our thoughts, emotions, and behavior. Policies, regulations, laws, and social guardrails can scarcely keep pace, much less overtake the myriad moral, ethical, legal, and socio-political dilemmas generated by the wide-spread commercial release of these systems.

A Report from the U.S. Homeland Security Operational Analysis Center² warned that “AI systems have the potential to destabilize social, governance, economic, and critical infrastructure systems, as well as potentially result in human disempowerment” and can amplify “existing catastrophic risks, including risks from nuclear war, pandemics, and climate change.”

Throughout history, the introduction of new technologies, no matter how well-intentioned, potentially beneficial, or seemingly benign, has also inevitably brought unforeseen abuses, malicious uses, and unintended consequences. At its simplest, any tool can be weaponized – implements invented for hunting, crafting, or building such as spears, bows, and hammers have been transformed from tools for sustenance and developing social infrastructure to instruments of warfare and destruction.

Debates about where responsibility lies or whom to hold accountable for harms and misuses of various tools and technologies seem irresolvable. The specious question of whether it’s guns that kill or the people shooting them has m lingered for decades. Similarly, AI’s most ardent proponents reject that computational systems are in themselves dangerous. Problems, they claim, are usually a consequence of exogenous factors such as misalignment, technophobia, derelict regulation, improper implementation, or are dismissed as acceptable engineering bugs that will eventually be worked out.

A well-established heuristic in systems engineering claims that the purpose of a system is what it does. This view suggests that when a system is operating out of alignment with its intended design any resultant unintended consequences — caused by users or other actors who misunderstand the system’s purpose — ought to be readily correctable. The system just needs to be returned to a state where it can do what it does.

While challenges to ideal implementation can certainly present externally to the system, there is strong evidence that many of the risks associated with introducing AI systems and services into society at scale are largely attributable to wild over-estimations of

² Global Catastrophic Risk Assessment. Homeland Security Operational Analysis Center. RAND Corporation, 2024. https://www.rand.org/pubs/research_reports/RRA2981-1.html. (accessed 1 July 2025)

their actual capabilities compounded by tech leaders' insatiable reach for power and wealth. AI is a human enterprise devised, driven, and shaped not only by experimentation and innovation, but by our hopes, fears, foibles, and fantasies. The root causes of most problems are invariably human, not technological.

This being said, AI represents a revolutionary category of human invention. It is not just another entry in the cannon of conventional widgets, services, or tools. It is not a spear or hammer, or even analogous to world-changing innovations like the wheel, electric light, vaccines or antibiotics. Unlike technologies conceived for purely utilitarian purposes, AI is the product of a unique mission to build "intelligent machines that could perform the most advanced human thought activities" as the Dartmouth Group proposed in the mid-1950s. It affects humanity as a whole and is being positioned, as I described in a 2019 article³ as a paradigm shift in the dominant principles governing human toolmaking and innovation: "our tools evolved from mechanisms of necessity to those which can assist us and enhance our lives to now outsourcing self-awareness, self-knowledge, and self-agency."

Not every tech product is intended to functionally replace human decision-making or provide a service we're supposed to experience as essentially human-like. But the ultimate aim of many frontier AI systems is to match or surpass human-level intelligence across a wide range of cognitive tasks, often referred to as Artificial General Intelligence ('AGI'), and to introduce machine agents that can operate autonomously in society in ways indistinguishable from humans.

In this regard, AI is a unique and unprecedented convergence of technology and psychology. It is a powerful technology designed to convincingly present as – functionally pretend to be – human.

The benchmark for assessing that capability is the Turing Test (originally referred to as The Imitation Game) developed in 1950 by Alan Turing, the renowned British mathematician and computer scientist often called the "father of modern computing," following publication of his ground-breaking paper *Computing Machinery and Intelligence*⁴ in which he posed the question, "Can machines think?" The test is intended to assess whether a machine could exhibit intelligent behavior equivalent to that of a human. A human evaluator judges a text transcript of a natural-language conversation between a human and a machine. The evaluator tries to identify the machine, and the machine passes if the evaluator cannot reliably tell them apart. The results would not depend on the machine's ability to answer questions correctly, but on how closely its answers resembled those of a human.

³ Stein, Alexander. Pitfalls of Outsourcing Self-Awareness to AI: What Leaders Need to Know. Forbes, Jan 6, 2019. <https://www.forbes.com/sites/alexanderstein/2019/01/06/the-pitfalls-of-outsourcing-self-awareness-to-ai-heres-what-leaders-need-to-know/> (accessed 1 July 2025)

⁴ Turing, Alan. Computing Machinery and Intelligence. *Mind: A Quarterly Journal of Philosophy and Psychology*, October 1950

In the mid-1960s, Joseph Weizenbaum, a German-American computer scientist working at MIT, developed an early natural language processing computer program he called ELIZA (after Eliza Doolittle, a working-class character in George Bernard Shaw's *Pygmalion* who is taught to improve her communication skills). Originally intended as a method to explore communication between humans and machines, it became one of the first programs capable of attempting the Turing test with many users attributing human-like feelings to it, a phenomenon that came to be called the Eliza effect. Despite Weizenbaum's insistence that ELIZA could not converse with true understanding, its ability to engage in fluent discourse convinced many early users that it possessed intelligence. Weizenbaum lamented that "ELIZA shows, if nothing else, how easy it is to create and maintain the illusion of understanding, hence perhaps of judgment deserving of credibility. A certain danger lurks there."⁵

While ELIZA is almost laughably rudimentary in comparison to today's large language model (LLM) chatbots, our willingness to suspend disbelief and impute prodigious human-ish capabilities which are in fact nonexistent is powerful.

In 1966, Weizenbaum presciently wrote:

*It is said that to explain is to explain away. This maxim is nowhere so well fulfilled as in the area of computer programming, especially in what is called heuristic programming and artificial intelligence. For in those realms machines are made to behave in wondrous ways, often sufficient to dazzle even the most experienced observer. But once a particular program is unmasked, once its inner workings are explained in language sufficiently plain to induce understanding, its magic crumbles away; it stands revealed as a mere collection of procedures, each quite comprehensible.*⁶

Then as now, we are beguiled by our impulses to anthropomorphize, be seduced by clever but misleading marketing propaganda that masks and misrepresents a slew of nontrivial capability deficiencies, and become lulled into accepting engineering achievements as independent thought and agency.

A 2024 experiment conducted by researchers out of UC San Diego suggests that people are increasingly challenged to distinguish GPT-4 from a human. Participants had a 5 minute conversation with either a human or an AI and judged whether or not they thought their interlocutor was human. GPT-4 was judged to be a human 54% of the time, outperforming ELIZA (22%) but lagging behind actual humans (67%). The results underscore that LLMs like GPT-4 perform language-based tasks at a level frequently experienced as at parity with humans. People interacting with these chatbots are unable to definitively determine whether they are speaking to a human or a

⁵ Weizenbaum, J. ELIZA: A Computer Program for the Study of Natural Language Communication Between Man and Machine. *Computational Linguistics* 9(1): 36-45 January 1966

⁶ Op. cit.

machine. The research⁷ provides what is claimed as the first robust empirical demonstration of an artificial system passing an interactive 2-party Turing test.

This experiment and others like it are interpreted to have implications for debates around machine intelligence and are generally taken to bolster claims that frontier computational systems are unequivocally on the verge of surpassing human capabilities in a range of areas. While this sort of research urgently – and correctly – suggests that deception by current AI systems may go undetected, it also tends to over-value the machine and subordinate the human as causal to that deception.

In my view, the Turing Test has never been about determining anything substantially meaningful regarding the capacity of a computer system but rather has always been an unscientific referendum on our omnipresent human susceptibility to being deceived. The test functions more like a Rorschach test in which the outcome is primarily indicative of the human evaluator's psychology and provides only notionally significant information about the capabilities or quality of the machine.

Following from this, what if the purpose of the test were, conversely, to try to ascertain the extent to which we can or cannot distinguish what or whom we're conversing with? The answer to that question could have value in returning important information about ourselves, for example, in creating protections against social engineering exploits, fraud, or other forms of deception and manipulation.

While AI applications can be directed to provide that sort of vulnerability feedback, the test's primary purpose remains determining how convincingly a machine can mimic human communication, in part, to gather training data to refine systems' future unsupervised deployment capabilities.

For technologists and computer scientists, crossing a Turing test threshold is a significant achievement. Not only is the system performing as intended, it further bolsters the aspiration of developing computational systems that exhibit intelligence equivalent to, greater than, or even indistinguishable from, a human.

Beyond intelligence – computational cognition – tech entrepreneurs are now intent on commercializing capabilities for artificial emotions and approximated empathy as more applications enter mainstream use and a familiar, trustworthy human-like interface is expected or required. Of primary additional importance in next generation agentic systems is the extent to which systems and services are perceived not only as safe and relatable to people interacting with them, but which foster instant rapport and thus can blur, perhaps eradicate, any conscious sense of interacting with a non-human entity.

⁷ Jones, C.R., & Bergen, B.K. (2024). People cannot distinguish GPT-4 from a human in a Turing test. ArXiv, arXiv:2405.08007

“Technology giveth and technology taketh away, and not always in equal measure. A new technology sometimes creates more than it destroys. Sometimes, it destroys more than it creates. But it is never one-sided.”

– Neil Postman

Will we develop systems and agents that can act and intervene in human affairs responsibly and fairly? Will nation states, governments, investors, commercial enterprises, private actors, judiciaries, legislatures, and other powerful stakeholders reach practical consensus on and be held accountable to violations concerning complex matters of international cooperation and governance, privacy, regulation, and legal, ethical, and other critical protections against and responses to abuses, misuses, and other harms? What are the consequences if we don’t or can’t?

Social communication and information networks running on advanced machine learning-based systems are already deeply embedded in our lives and are susceptible to both unwitting and deliberate abuses and misuses. User data – our most private and intimate details as well as banking or other data signatures and credentials – are regularly shared with companies, institutions, data brokers, and other third parties. Often, there’s no clear responsible party or agency for safeguarding the PII (Personally Identifiable Information) the systems harvest nor have robust legislative, legal, or regulatory mechanisms or AI data governance guidelines yet been broadly adopted to mitigate material and human risks or to provide equitable avenues for redress for harms caused.

We are, in my view, very far from overcoming the challenges of ensuring that the objectives and purposes of computational systems are compatible with and supportive of human values, goals, and preferences. To bad actors and criminal enterprises, this is good news.

Fraudsters are using AI-based techniques that traditional systems can no longer adequately detect or repel. Generative AI offers seemingly endless potential to magnify the nature and scope of fraud against financial institutions and their customers.

The availability of new generative AI tools is democratizing fraud. The dark web boasts a thriving cottage industry that sells scamming software to bad actors who can now easily and cheaply make deepfake videos and audios, and fictitious documents. AI’s automation capabilities are transforming the efficiency of criminal operations. The emergence of fully autonomous AI could usher a new era in organized crime, enabling malevolent actors to execute complex orchestrated attacks by identifying multiple vulnerable targets, hijacking their systems, and stealing valuable data from unsuspecting victims at scale, to launch massive money-laundering or trafficking operations, or exploit socio-political events for corrupt aims.

A 2024 report from Deloitte’s Center for Financial Services predicts that by 2027, GenAI could enable fraud losses in the United States to reach US\$40 billion, up from

US\$12.3 billion in 2023, a compound annual growth rate of 32%. In the last three years, deepfake attacks increased a staggering 2,137%, representing 1 in 15 cases of all fraud attempts detected⁸.

Hostile nation-states and mercenary adversaries aiming to disrupt elections or destabilize geopolitical affairs and transglobal commerce are likewise gaming AI to spread propaganda or push false or inflammatory information. Because chatbot answers depend on and reflect the data fed into them, the responses they give users can be manipulated by infecting the datasets with intentionally skewed or false information.

In these situations, AI systems are weaponized in ingenious and creatively malevolent but still fundamentally conventional ways: as a malicious tool. The system's vulnerabilities are deliberately exploited to force the system to do what the malicious actors want it to; what it was supposed to do be damned. Sysadmin restrictions and other safeguards or countermeasures are supposed to protect against such nefarious acts, although wily actors understand how to defeat these by identifying blind spots and weaknesses.

But adoption or willful misuse of cutting-edge technologies for the knowing commission of nefarious or unlawful activities is, as alluded to earlier, entering an altogether different dimension. Frontier AI can now so effectively deceive us that trust in consensual agreement of validated truth and reality is being functionally eradicated. Advancements in AI blur the line between reality and fabrication, challenging our trust not just in digital content but in reality itself, including knowing or caring who is human or not.

"The point of modern propaganda isn't only to misinform [but] to annihilate truth."

– Garry Kasparov

We have willingly allowed a powerful but still largely unproven technology to be integrated into nearly every strata of society, commerce, and human affairs.⁹

There is a growing body of social science research demonstrating that many AI-based systems and services are adversely impacting children's psycho-social development and hamstringing kids' abilities to learn and think critically, even as companies market and sell AI tools and services into the education and mental health marketplace. Technologies that appeared (or were hoped) to be solutions to the adolescent and

⁸ Lalchand, Satish; Srinivas, Val; Maggiore, Brendan; Henderson, Joshua. Generative AI is expected to magnify the risk of deepfakes and other fraud in banking. (29 May 2024). Deloitte Center for Financial Services

<https://www2.deloitte.com/us/en/insights/industry/financial-services/financial-services-industry-predictions/2024/deepfake-banking-fraud-risk-on-the-rise.html>

⁹ Stein, Alexander. What AI Can and Can't Do and How Psychoanalysis Can Help. The CAI Report, Issue 1 | January 2025 <https://apsa.org/what-ai-can-and-cant-do/>

young adult mental health crisis following the Covid pandemic, are now being understood as causal to, not reparative of, increases in isolation, loneliness, anxiety, depression, self-harm, and suicidality.

Advances in GenAI's capabilities have also given rise to issues involving what MIT sociologist Sherry Turkle discusses as the “perils of pretend empathy and artificial intimacy.”¹⁰ Not merely over-the-horizon conceptual challenges, these are currently iterated in real-world commercial ventures. There is already a robust profit-driven market sector producing sex-bots – sophisticated life-like artificial sex partners – and death-bots (also referred to as griefbots) – avatars that recreate the appearance, speech, and primary personality features of a deceased person.

There are now chatbot “therapists” and a wave of other related mass-market applications purporting the capability of diagnosing and responding to depression, anxiety, relationship travails, and various other mental health issues. Other chatbot services can generate human-like text responses based on a user's customization to provide “realistic conversations” with AI-generated personas. The technology is presented to encourage – manipulate may be the more accurate word – us into believing that we can have relationships with it, and it with us — as depicted in the films “Ex Machina” (2014) and “Her” (2013) — in ways functionally and emotionally equivalent, possibly even superior, to those with other people.

All of which leads me to suggesting that we can plausibly consider AI as an imposter – meaning, the assumption of a false or disguised identity to deliberately deceive – a perspective adjacent to the philosopher and cognitive scientist Daniel C. Dennett's caution against the problem of “using AI to generate counterfeit people.”¹¹

A deep dive into the conceptual details and psycho-social complexities of what I call techno-imposturousness will need to wait. I only want to quickly spotlight here the bilateral, relational nature of this issue. Fraud, as I pointed to at the beginning, pivots on relationships. But now, we are entering uncharted territory where the fraudster is not a person but a computational system.

On closer examination, the culprit, the true agent and instrument of deception, is more properly understood to be the technology industry and, in particular, a relatively small group of individuals -- the principal innovators, investors, tech and business leaders, and others in Silicon Valley whose personal beliefs, ideologies, and psychological proclivities in pursuit of a techno-utopian vision of the future¹² -- who are guiding

¹⁰ Turkle, Sherry. 2024. “Who Do We Become When We Talk to Machines?” An MIT Exploration of Generative AI, March. <https://doi.org/10.21428/e4baedd9.caa10d84>.

¹¹ Dennett, Daniel C. The Problem with Counterfeit People. The Atlantic, May 16, 2023. <https://www.theatlantic.com/technology/archive/2023/05/problem-counterfeit-people/674075/> (accessed 1 July 2025)

¹² A set of ideologies known as TESCREALism, an acronym which denotes “transhumanism, Extropianism, singularitarianism, (modern) cosmism, Rationalism, Effective Altruism, and longtermism” per Gebru, Timnit and Torres, Émile P. The TESCREAL bundle: Eugenics and the

concept, design, research and development, operationalization, and commercialization.

These tech evangelists promise magical solutions just as medieval alchemists believed the Philosopher's Stone could transform base metals into gold.

Trust cannot be broken unless it is first given. AI's high-velocity ascent is to a large degree driven by our collective acceptance of its anthropomorphized presentation, strategically enabled by the relentless delivery of savvy marketing propaganda masquerading as validated science. We have been given to accept that machine-generated simulacra of something human-like is not only good enough but absolutely equivalent. Imposturousness cannot succeed, no matter how brilliantly it's executed, unless its victims agree to mistake or deny appearance for actuality. Society has been groomed to enable what may come to be understood as the most far-reaching and consequential fraud in history.

How does this happen? "People," Professor Dennett says, "have a natural inclination to treat anything that seems to talk sensibly with us as a person ... almost impossible to resist."¹³

Referencing Dutch historian Johan Huizinga's idea of the "magic circle"¹⁴ – the space in which the normal rules and reality of the world are suspended and replaced by the artificial reality of a game world – Edward Castronova, a professor of media at Indiana University Bloomington known for his work on the economies of synthetic worlds, suggests that "the membrane between synthetic worlds and daily life is porous ... [and that] people are crossing it all the time in both directions, carrying their behavioral assumptions and attitudes with them."¹⁵

In a recent article elaborating key distinctions between human and computational thought¹⁶, I suggested that the project to engineer intelligent machines has always been linked to an idealized fantasy of pure cognitive decision-making. We are, it would seem, enthralled by the wish for a perfect brain-in-a-vat unburdened by the needs and challenges of the physical body and devoid of affect, irrationality, fallibility, vulnerability, pain, memory, or other vicissitudes of the human condition. Ambivalence and hostility toward our physical and emotional selves—the drive to eradicate or replace ourselves with an "improved" version—is woven into the history

promise of utopia through artificial general intelligence. First Monday, Volume 29, Number 4 - 1 April 2024 DOI: <https://doi.org/10.5210/fm.v29i4.13636>

¹³ Dennett, Daniel C. Op. cit.

¹⁴ Huizinga, Johan. *Homo Ludens: A Study of the Play-Element in Culture*. 1938

¹⁵ Castronova, Edward. *Synthetic Worlds: The Business and Culture of Online Games*. University of Chicago Press, 2005

¹⁶ Stein, Alexander. *Computation Is Not Mentation: Why embodiment and lived experience matter*. The American Psychoanalyst, March 20, 2025

<https://americanpsychoanalyst.substack.com/p/computation-is-not-mentation/> / <https://tinyurl.com/mscdzsjw>

of civilization. Synthetic super-intelligent entities along with humanoid robots, cyborgs, and other human-like surrogates have long been an appealing leitmotif in sci-fi as a 'solution' to the 'problem' of being human. Once the stuff only of writers' and filmmakers' imaginations, they are now commonplace in the real world.

But what have we done in being able to actualize that? Magical thinking and willful blindness — mental devices in service of attempting to stamp out something in reality that feels overwhelming — conjoin. In "Remembering, Repeating, and Working-Through," published in 1914¹⁷ (and elaborated in his 1920 book "Beyond the Pleasure Principle"), Freud identified our propensity for making and remaking the same mistakes over and over again. We are infinitely resourceful in recreating old problems in new ways, thinking that we're solving them without realizing we're not only preserving the original but often also creating a new one.

Techno-imposturousness isn't equivalent to a Trojan horse, a boiler room, Nigerian prince, or charlatan's grift. We are drowning in an ocean of fakery, a digitally conjured facsimile of water in a virtual world populated with computer-generated avatars. We have apparently decided and declared that all of that is real. Or approximately real enough. It is not. But the consequences are unavoidable and irrevocable. Being defrauded by our own invention is entirely self-generated and self-inflicted. The problem is not technology. It is us.

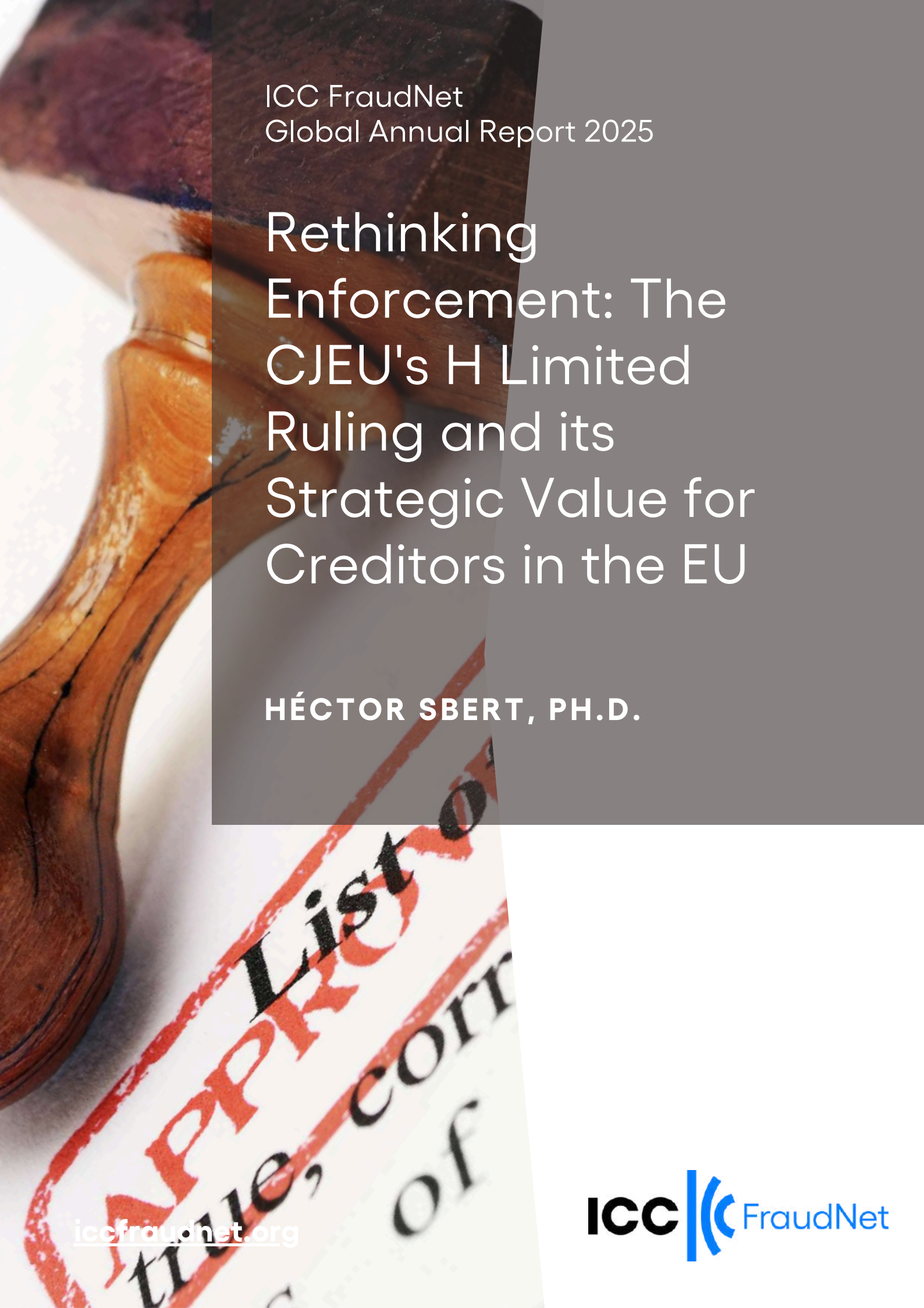
¹⁷ Freud, S. Remembering, Repeating and Working-Through (Further Recommendations on the Technique of Psycho-Analysis II) in The Standard Edition of the Complete Psychological Works of Sigmund Freud, 12(0):145-156, 1914

ICC FraudNet
Global Annual Report 2025

Part II: Enforcement and Regulation

iccfraudnet.org





ICC FraudNet
Global Annual Report 2025

Rethinking Enforcement: The CJEU's H Limited Ruling and its Strategic Value for Creditors in the EU

HÉCTOR SBERT, PH.D.

iccfraudnet.org

ICC  FraudNet



Rethinking Enforcement: The CJEU's *H Limited* Ruling and its Strategic Value for Creditors in the European Union

**Héctor Sbert Ph.D.
ECIJA**

Introduction

For practitioners dealing with cross-border disputes, the recognition and enforcement of non-EU judgments has often been a source of delay and uncertainty. The CJEU's ruling in *H Limited* (C-568/20) offers a potentially game-changing interpretation: a judgment issued in an EU Member State that enforces a third-country decision may itself be recognised and enforced throughout the EU under Brussels Ia. This opens strategic opportunities for creditors who might otherwise face fragmented national barriers.

The recognition and enforcement of third-state judgments—those issued by courts outside the EU—has long posed legal and practical challenges. With the UK's withdrawal from the European Union, one might have expected the impact of English court decisions to recede within the EU framework. Yet the Court of Justice of the European Union (CJEU), in its landmark and controversial *H Limited* decision, appears to have reopened a backdoor for third-country judgments to enter the EU's judicial space.

This article explores the legal reasoning and practical consequences of the *H Limited* ruling, a landmark step that could help facilitate the recognition and enforcement of

third-country judgments within the EU. While some voices in the academic debate have raised concerns, the decision opens up new avenues for judgment creditors to access EU enforcement mechanisms through innovative litigation strategies. Building on the relevant case law, this piece examines how *H Limited* redefines enforcement opportunities post-Brexit and how Member States can adapt to this evolving landscape.

Legal Background: The Hard Border of Brussels Ia

The Brussels Ia Regulation (Regulation (EU) No. 1215/2012) sets out a unified regime for the recognition and enforcement of judgments across EU Member States. Article 36(1) provides for automatic recognition, and Article 39 allows for enforcement without any special procedure—so long as the judgment was rendered in a Member State.

By contrast, judgments from non-EU countries must be recognized and enforced under national law. This often involves an exequatur procedure and compliance with additional conditions: international jurisdiction of the foreign court, due process, absence of public policy violations, and sometimes reciprocity.

Historically, the CJEU held in *Owens Bank* (C-129/92) that enforcement decisions concerning judgments from third states did not fall under the Brussels regime. This reflected a consensus that ‘*exequatur sur exequatur ne vaut*’—that is, a judgment enforcing a non-EU judgment could not itself circulate under Brussels Ia.

The Decision in *H Limited*

In *H Limited*, the CJEU held that an English “confirmation judgment”—a judgment rendered by the English High Court confirming a Jordanian judgment—qualified as a judgment under Article 2(a) of the Brussels Ia Regulation and was thus subject to automatic enforcement in Austria.

The English confirmation judgment had been rendered after adversarial proceedings. The English court did not examine the merits of the Jordanian judgment but verified its finality, jurisdiction, and compatibility with English public policy.

The CJEU emphasized the Regulation’s goal of ensuring the free circulation of judgments and held that the nature or origin of the claim was irrelevant, provided the judgment had been or could have been issued through adversarial proceedings.

This broad reading raised concerns among scholars and practitioners alike: would this allow creditors to transform unenforceable non-EU judgments into EU judgments through Member States like England?

Strategic Enforcement Opportunities Post-*H Limited*

Instead of framing *H Limited* as a loophole or risk, legal practitioners should consider its utility. The decision enables parties to obtain a local confirmation judgment in a Member State with favorable procedures—such as Ireland or the Netherlands—and use it as a springboard for EU-wide enforcement. This is particularly valuable in cases where direct exequatur might be unavailable or impractical. In an age of asset mobility, creditors need access to fast and effective enforcement paths. *H Limited* makes that possible.

The *H Limited* decision has been met with lively academic discussion. While it departs from the earlier precedent in *Owens Bank*, many view it as a pragmatic recognition of evolving litigation realities in a globalised legal environment. The ruling enables creditors to overcome the fragmented and often uncertain procedures for enforcing third-country judgments in the EU by using Member States that convert such judgments into new domestic titles. Rather than undermining the Brussels Ia regime, this may be seen as harmonising outcomes and promoting access to justice through practical solutions.

Of course, some commentators have raised concerns about potential abuse—such as 'judgment laundering' or the use of a 'Trojan horse' strategy to gain enforcement in stricter Member States via more lenient ones. However, these risks should be balanced against the need for cross-border commercial certainty and creditor protection. In a post-Brexit legal landscape, providing mechanisms for effective enforcement of foreign judgments is both timely and aligned with the EU's broader goals of judicial cooperation and efficiency.

Even though the UK is no longer part of the Brussels Ia system, *H Limited* remains relevant. The mechanism it validated may now be replicated in other Member States with similar procedural frameworks.

The Two Conditions for *H Limited* to Apply

For a national enforcement decision to fall within *H Limited*'s scope under Brussels Ia:

- It must be a new judgment on the foreign debt, not merely a declaration of enforceability (i.e., not an exequatur); and
- It must result from (or be capable of) adversarial proceedings.

This means the decision must involve a genuine judicial assessment, albeit limited, of the enforceability of the foreign judgment, with an opportunity for the debtor to be heard.

Candidate Jurisdictions for Enforcement 'Through the Backdoor' after Brexit

Tobias Lutzi¹ identifies four such jurisdictions:

1. *Ireland*: Irish courts enforce foreign money judgments through an action on the judgment debt. The process is adversarial and closely resembles the English method. This makes Ireland an attractive venue for crafting an EU-compatible judgment.
2. *Cyprus*: Following common law, Cypriot courts allow actions on foreign judgments, though enforcement is generally limited to debtors resident in Cyprus.
3. *Netherlands*: Dutch law requires a new action under Article 431(2) CCP when no treaty applies. The Dutch Supreme Court's *Gazprombank* ruling allows recognition of a foreign judgment as *res judicata*, leading to a new enforceable Dutch judgment without reviewing the original merits.
4. *Sweden*: In limited cases, particularly where there is a jurisdiction agreement, Swedish courts may render a new decision based on a third-country judgment, provided due process was observed.

The Role of Public Policy and Procedural Safeguards

While the CJEU invoked the public policy exception in Article 45 Brussels Ia as a safeguard, such mechanisms should be viewed as fallback protections rather than barriers to enforcement. The reality is that confirmation judgments, though based on third-country decisions, go through judicial review—however limited—and reflect a modern approach to balancing procedural safeguards with enforcement efficiency.

Rather than weakening national control, the system preserves key safeguards by allowing Member State courts to reject enforcement where core principles are violated. However, in most cases, courts are well-positioned to assess the enforceability of these judgments and support the free movement of justice across borders.

But this safeguard may prove ineffective. If the confirming court does not examine the substance (as is typical in confirmation judgments), the debtor's only remedy is to raise a public policy objection—shifting the burden of proof and undermining national control over foreign judgment enforcement.

¹ Lutzi, T. (2024). What remains of *H Limited*? Recognition and enforcement of non-EU judgments after Brexit. *Journal of Private International Law*, 20(3), 651–667.
Available at: <https://doi.org/10.1080/17441048.2024.2439152>

Implications and Outlook

H Limited represents a significant step forward in enabling the effective enforcement of third-country judgments within the EU. For judgment creditors, it creates a pragmatic route to convert judgments into enforceable titles within the internal market—without excessive duplication of legal proceedings.

This new pathway empowers parties who may otherwise face dead ends in enforcement due to fragmented national regimes. Rather than undermining legal coherence, it contributes to the progressive adaptation of EU private international law to transnational economic realities.

Looking ahead, Member States may wish to clarify procedural criteria, but the core opportunity created by *H Limited*—facilitating legitimate enforcement in complex international cases—deserves to be embraced.

This raises complex questions:

- Should EU law permit such indirect enforcement of third-country judgments?
- Does the Regulation’s mutual trust principle extend to judgments enforcing non-EU judgments?
- Is further legislative reform required to clarify the scope of Brussels Ia?

Hypothetical Scenarios: Strategic Use of *H Limited*

To better understand how the *H Limited* ruling might be used in practice, it is helpful to consider two hypothetical case studies:

Scenario 1: Enforcement via Ireland

A creditor obtains a final and conclusive money judgment from a Canadian court. The debtor holds assets in Germany but is unlikely to satisfy the judgment voluntarily. Instead of seeking recognition directly in Germany—where exequatur requirements may pose challenges—the creditor initiates an action on the judgment in Ireland. The Irish court, applying common law principles, renders a new Irish judgment confirming the Canadian debt. Armed with this EU judgment, the creditor seeks automatic enforcement in Germany under Brussels Ia.

Scenario 2: Judgment Shopping in the Netherlands

A U.S. investor wins a judgment in New York against a French defendant but faces resistance in French courts due to procedural objections. The investor initiates proceedings in the Netherlands under Article 431(2) CCP. The Dutch court, recognizing the finality and enforceability of the U.S. judgment, issues a new Dutch

decision granting the same relief. This Dutch decision, now an EU judgment, is enforced in France under Brussels Ia, bypassing domestic barriers.

These examples illustrate the strategic potential unlocked by the *H Limited* precedent. While national courts retain control through public policy exceptions, the decision invites creative litigation planning and challenges Member States to harmonize their responses to third-country enforcement strategies.

Doctrinal Debate and Legislative Perspectives

The doctrinal response to *H Limited* reflects a healthy debate about the future of enforcement within the EU. While some scholars advocate for caution, many practitioners see the decision as a welcome development that aligns legal practice with the realities of cross-border commerce and dispute resolution.

Rather than calling for restriction, some voices suggest harmonisation—ensuring that all Member States apply consistent criteria when converting third-state judgments into domestic ones. This could involve legislative fine-tuning or broader adoption of instruments like the 2019 Hague Judgments Convention.

Ultimately, the decision provides an opportunity to modernise EU law while safeguarding fairness, due process, and mutual trust across jurisdictions.

From a doctrinal standpoint, the CJEU's expansive reading of Article 2(a) Brussels Ia has been accused of conflating form with substance. A judgment, under Brussels Ia, should arguably reflect a determination of rights and obligations under EU or Member State law, not a procedural validation of a third-country decision. This concern is particularly acute considering procedural disparities across jurisdictions. For example, a summary judgment based on *res judicata* may not guarantee the same level of procedural fairness or substantive review as a full *exequatur*.

These concerns have led some scholars and practitioners to call for legislative clarification. One option would be to amend Article 2(a) to explicitly exclude judgments that are based solely on foreign decisions. Another would be to create a distinct mechanism—akin to an enhanced *exequatur*—for recognising such hybrid judgments, with safeguards tailored to address public policy and procedural equity. Furthermore, the Commission could consider a new initiative for harmonising the recognition of third-state judgments, inspired by international instruments such as the 2019 Hague Judgments Convention. Though the EU has signed the Convention, its implementation remains pending. Aligning Brussels Ia with Hague standards could offer a more coherent, transparent, and mutually respectful approach to cross-border recognition and enforcement beyond the EU.

Comparative Insights and Future Litigation Risks

From a comparative standpoint, *H Limited* reflects global best practices in judgment enforcement. Jurisdictions like Ireland and the Netherlands have long allowed actions on foreign judgments. Rather than promoting forum shopping, this flexibility strengthens the overall enforceability of international claims, enabling commercial actors to recover debts efficiently.

Rather than creating litigation risk, the decision highlights the need for proactive strategy. Creditors and their counsel must now consider a broader set of enforcement tools, including jurisdictional planning and asset targeting. This fosters a more integrated legal space, where legitimate claims can be pursued with confidence across borders.

National courts remain fully empowered to filter abusive cases through existing legal safeguards. The key message of *H Limited* is not vulnerability, but opportunity—if supported by thoughtful legal design.

Moreover, the asymmetry between the recognition of intra-EU and third-state judgments raises concerns about legal predictability. A judgment creditor may, by exploiting favorable national laws, gain access to EU-wide enforcement without undergoing the substantive scrutiny required in the target jurisdiction. Such inconsistencies can disproportionately impact debtors, particularly in states with stricter procedural safeguards or different views on international jurisdiction.

From a litigation risk perspective, *H Limited* complicates cross-border asset protection strategies. Debtors may now face enforcement actions in jurisdictions they did not anticipate, initiated through indirect pathways. Litigants must increasingly monitor not only the original foreign proceedings but also any secondary enforcement attempts in Member States susceptible to confirmation-based recognition.

Practitioners must therefore advise clients not only on the merits of the primary case, but also on the enforcement landscape within the EU. Due diligence should include a mapping of potential Member States where a third-state judgment could be converted into an EU judgment. Strategic pre-litigation planning, including asset location analysis and jurisdictional risk assessment, will be more critical than ever.

Finally, given the CJEU's reluctance to restrict the formal definition of 'judgment', national courts may need to play a more active role in applying public policy exceptions under Article 45 Brussels Ia. This creates an opportunity—and a burden—for Member State courts to safeguard procedural integrity while respecting the spirit of mutual recognition.

Conclusion

H Limited offers a pragmatic route for judgment creditors navigating the post-Brexit enforcement landscape. While safeguards such as public policy exceptions remain in place, the ruling encourages creditors to take a proactive, cross-jurisdictional approach. Legal advisors should include *H Limited*-based strategies in their enforcement playbook—especially when non-EU judgments are involved and strategic asset recovery across the EU is on the table.

The *H Limited* ruling signals a new chapter for the enforcement of third-country judgments in the EU. Rather than fearing its consequences, stakeholders should see it as a practical and principled evolution of the Union's private international law framework.

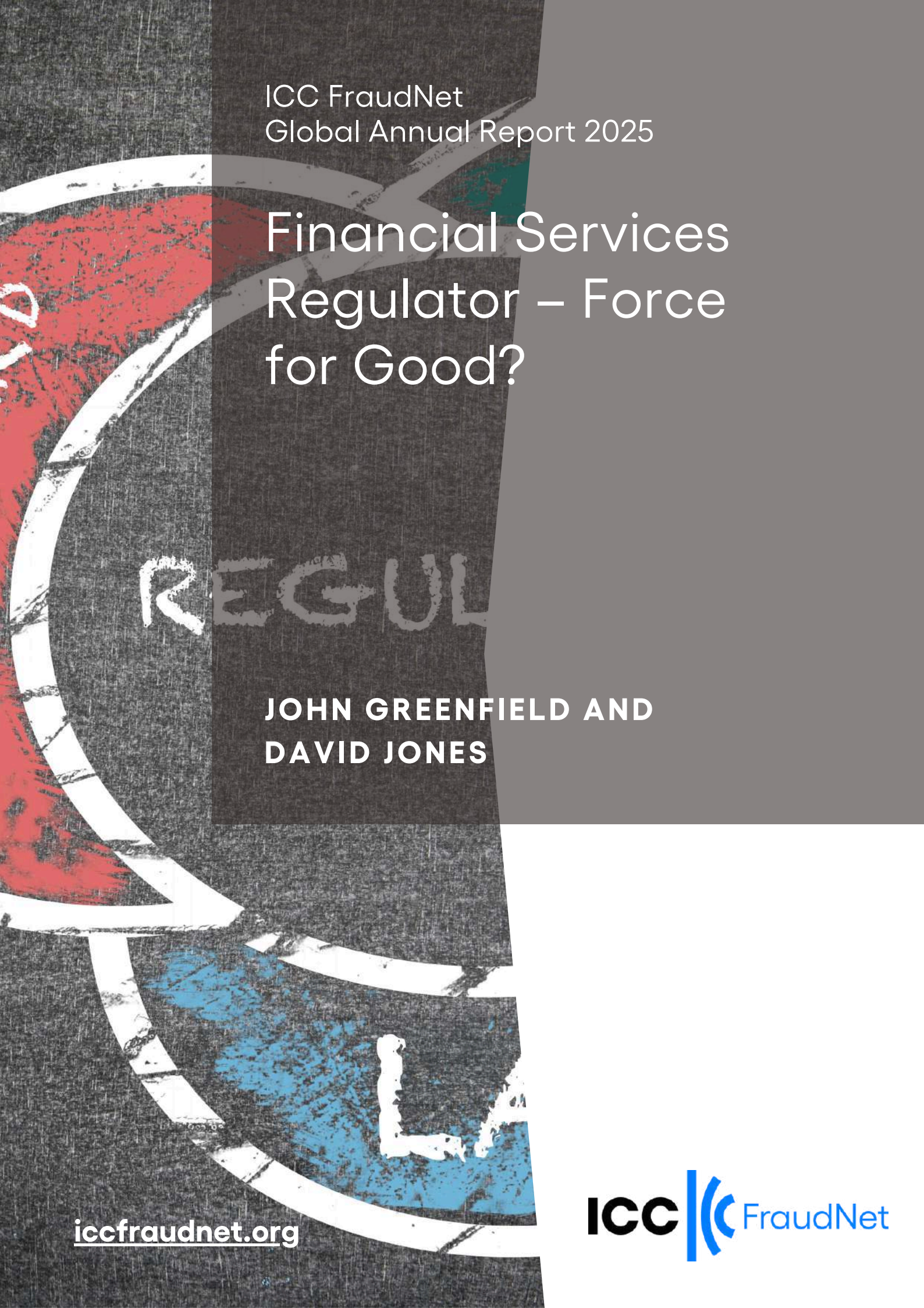
Judgment creditors now have greater clarity and access to enforcement mechanisms. This enhances legal certainty, promotes efficiency, and aligns with the cross-border realities of modern commercial litigation.

With appropriate procedural safeguards in place, and possible future legislative refinements, *H Limited* has the potential to serve as a model for integrating external judgments into the EU's internal legal space.

Judgment creditors, especially after Brexit, may continue to exploit this route through carefully selected jurisdictions. Whether this amounts to 'judgment laundering' or practical legal strategy depends on one's view of legal coherence and the integrity of EU private international law.

Further judicial and legislative clarification is needed. Until then, *H Limited* remains a powerful—if controversial—tool in the arsenal of transnational enforcement.

This article examines the practical implications of the CJEU's decision in *H Limited*, a case that reshapes how non-EU judgments can be enforced across the European Union. Rather than a purely academic controversy, *H Limited* offers real-world tools that litigators and creditors can deploy to navigate complex enforcement environments. With post-Brexit uncertainties still unfolding, this decision opens new possibilities for accessing the EU enforcement framework via Member States that convert foreign judgments into domestic orders.



ICC FraudNet
Global Annual Report 2025

Financial Services Regulator – Force for Good?

**JOHN GREENFIELD AND
DAVID JONES**

iccfraudnet.org





Financial Services Regulator – Force for Good?

**John Greenfield, Mourant and
David Jones, Carely Olsen¹**

The writer arrived in the Bailiwick of Guernsey in January 1981 to commence work as a lawyer in its then fledgling finance industry. At that time, the idea of a full-time independent Regulator (let alone a fully staffed regulatory department!) was still far off. That's not to say there were no regulations. For example, Exchange Control regulations (requiring approval of the Bank of England for the removal of funds from Guernsey) had only just come to an end.

Fast forward to today, after decades of statutory regulatory growth and the development of the Guernsey Financial Services Commission ('the Commission') dedicated to an effective enforcement of all regulations governing each sector of the finance industry with dedicated departments fully staffed with highly trained specialists given extremely wide powers of inspection, enforcement and sanctions for breaches.

However, an issue that has arisen and been considered in a number of recent cases in the Guernsey Courts is how the statutory regime (and therefore the powers that are available to the Commission) should be exercised and, in particular, whether there is any tension between basic Human Rights principles (Guernsey being a signatory to the Convention on Human Rights) and the statutory process.

The Commission was created by statute (the Financial Services Commission (Bailiwick of Guernsey) Law 1987) and its powers have been updated at various times since the

¹ With grateful thanks to 4 New Square Chambers, Strategic Partner of ICC FraudNet.

Financial Services Business (Enforcement Powers) Bailiwick of Guernsey Law 2008.

The Regulations (and powers) govern the whole range of financial services including protection of investors, fiduciaries, insurance (including managers and intermediaries), banking, and collective investment schemes.

These statutes combined require the Commission to take such steps as it considers necessary or expedient for the effective supervision of finance business in the Bailiwick of Guernsey. It also has a role in countering financial crime and the financing of terrorism and is required to take steps for maintaining competence in Guernsey's financial services sector and the safety, soundness and integrity of the sector. It is required to protect and enhance Guernsey's reputation as a finance centre. The robust statute enables it to do anything which appears to it to be conducive to the carrying out of its functions or to be incidental to their proper discharge.

As can be seen, its powers are very wide indeed. When exercised, they can easily lead to the end of someone's career.

In addition, its enforcement powers allow it to impose discretionary financial penalties (now up to £400k), up to lifetime bans for carrying on any regulated activities and to publish for public information any statements relating to its findings and sanctions imposed – which can be against a company/licensee and its relevant officers.

These powers are not unusual in the modern world of regulation, but the question arises what limitations, restrictions or suspensions may apply to the exercise of these wide powers and what consequences might flow when the Commission gets it wrong. It is only human!

Before delving into the numerous Court decisions involving the Commission, it is worth noting that there are numerous other aspects of everyday life. One such example concerns the working of the Guernsey Competition and Regulatory Authority ('GCRA') which has a counterpart in many other jurisdictions now. In Guernsey, it was established in 2012 with statutory powers to intervene (and, if necessary, sanction any aspect of conduct which may be regarded as anti-competitive). In Guernsey, the provision of specialist medical care is carried out through a medical partnership called the Medical Specialist Group ('MSG'). The GCRA determined that provisions in the partnership agreement requiring all partners to sign up to restrictive covenants breached the anti-competitive regulations. MSG appealed as it was entitled to through the island's Royal Court, presided by a judge sitting alone.

The case really turned on its own facts as to whether the restrictive practices could (and whether they actually did) result in anti-competitive consequences – particularly where they prevented a partner who left the MSG from working in the island for a certain period.

A number of legal principles were laid down. For example, does the fact that GCRA could impose financial sanctions on the MSG mean the proceedings were criminal or quasi-criminal for the purposes of Act 6 of the European Convention on Human Rights?

In consequence, there would be a requirement for the Appellate Court to carry out a full merits review involving effective and thorough judicial scrutiny of any findings of fact made by GCRA.

In this case the Court ruled that as a result of significant financial penalties available, the criminal jurisdictional elements of Article 6 ECHR are engaged. Accordingly, it further ruled that the appeal gave the Court full jurisdiction (merits review).

In addition, the Court made the following findings: -

1. The burden of proof to establish its case remained with the Regulator;
2. On the facts of this case, the findings were not established;
3. On the process established by statute, and the fact that certain facts needed further review, the case would have to be remitted back to the GCRA for reconsideration; and
4. Costs will follow the event (i.e. paid by GCRA).

This follows a number of cases – perhaps the most important of which was heard before the Court of Appeal in Guernsey in February 2025 and of which judgment remains eagerly awaited, called *Fuller and Others v. GFSC* ('Fuller'). Carey Olsen appeared for one of the four appellants in this case and one of FraudNet's Strategic partners – 4 New Square Chambers – provided invaluable support. In the previous year, the Court also ruled upon the case of *Weighbridge Trust Ltd v. GFSC* ('WTL') and *Domaille and Others v. GFSC* ('Domaille').

WTL was principally concerned with the GFSC's power to publish on its website a "public statement" giving appropriate details of its findings (which could range from dishonesty to incompetence of a director/officer and the financial or other sanctions imposed). Obviously, such publication can have the effect of ending a career. WTL reviewed arguments over whether such publication was "reasonable" and/or in "the public interest". The company concerned, which conducted regulated financial business, had a complete new set of directors and other officers since the original activities complained of which had caused the GFSC to impose sanctions. The GFSC nevertheless wanted to issue a public statement which would be damning for its business and thereby penalise the new directors who had taken no part in the bad conduct. The argument was that even *if* a leopard cannot change its spots, a company *can* change its board of directors. The Court had to consider whether it was unreasonable in all the circumstances of the case to issue the public statement. The judge decided that on the facts it was indeed unreasonable and the decision by the GFSC was set aside. The Regulator had a duty to take all reasonably possible steps to

avoid or at least minimise "collateral damage" to innocent third parties (whilst not prejudicing any applicable parties' interest).

The Domaille case is potentially going on to appeal to the European Court, but the rest of this article will focus on the Fuller case (on which judgment is still awaited). This case has a particular interest because it is the first case which has really applied detailed scrutiny to the whole GFSC power as it operates in Guernsey and especially from a Human Rights perspective.

The case involved a fraud perpetrated on investors by fraudsters based in Miami and Brazil resulting in losses exceeding £37m. Guernsey companies were utilised to promote the fraud, but it was always accepted that the Guernsey resident directors and officers were not parties to the actual fraud itself and did not benefit from it – receiving only the standard financial benefits from their office. Indeed, some of the Guernsey defendants invested their own money into the scheme – essentially a Ponzi scheme. Nevertheless, the GFSC commenced an investigation and after that was complete, they handed over their findings to a Senior Decision Maker ("SDM") in this case a KC based in London. The difficulty here is that under this system, the SDM is appointed by the GFSC, paid by the GFSC and becomes temporarily a part of it – indeed he signs off "for the GFSC" on his report. He supported all the GFSC's recommendations and notably found at least one of the defendants to be lacking credibility in their representations. He recommended severe penalties, including fines and (in some cases) lifetime prohibitions from working in the regulated sector of finance business. The defendants appealed to the Royal Court (judge sitting at first instance). The immediate difficulty was that although the adverse findings did not extend to participation in the fraud itself, they did extend to finding serious fault in complying with the duties applying to directors/officers of a company and lack of integrity and competence (in some cases amounting to dishonesty). However, the Royal Court considered itself limited in its appellate jurisdiction so that it could not overturn findings of fact by the SDM.

The Human Rights arguments therefore centred around whether the Appellants had ever faced a hearing presided over by a wholly independent tribunal. Could the SDM in reality be considered independent given his connection with the GFSC. This was a critical issue as it was submitted by the GFSC that the Royal Court itself did not have the power to conduct a full merits-based trial *de novo* or to assume a primary fact-finding function. Instead, the GFSC argued that an English KC, by training and experience, could be assumed to be able to act and carry out his functions in an "independent" way and would not be influenced by his relationship from the outset with the GFSC. Otherwise, the process may well not be compliant with the requirements of Article 6, ECHR.

One other interesting issue was that the GFSC argued that even if it lost the case, it should be immune from having any costs order against it. Given the high costs suffered by the Appellants to achieve any exoneration, this would be a considerable blow. The

GFSC argue that it cannot fulfil its statutory functions if it has the fear of losing costs hanging over it. In Guernsey, the GFSC raises the funds it needs from charging the finance sector license fees to carry on regulated business. Again, this will be a very interesting issue for the Court to tackle.

There were many other complex issues to be adjudicated on by the Guernsey Court of Appeal – too numerous to address in this article, but the recorded judgment – due any day now – will attract great interest in many financial jurisdictions and may have considerable impact on the supervisory powers of the Regulator – both in Guernsey and elsewhere.

Watch this space!



ICC FraudNet
Global Annual Report 2025

Navigating Regulatory Challenges: Crypto Compliance in the Digital Asset Era

JAVIER ALVAREZ

iccfraudnet.org





Navigating Regulatory Challenges: Crypto Compliance in the Digital Asset Era

Javier Alvarez
BDO

In recent years, the digital asset landscape has transformed significantly, driven by heightened regulatory scrutiny and deeper integration into mainstream financial services. Innovations such as decentralized finance (DeFi) and new cryptocurrency tokens continue to reshape the market, challenging regulators to create frameworks that balance innovation with financial stability and consumer protection. The rapid evolution of the crypto market has prompted a shift from a passive regulatory stance to proactive compliance measures. Initially, many regulators adopted a ‘wait-and-see’ approach, but incidents of fraud and market manipulation have accelerated the need for stringent oversight.

The global nature of the crypto industry presents significant jurisdictional challenges, as many firms operate without a physical presence in any single country. This situation complicates the determination of which regulatory body holds prominence and how to prevent regulatory arbitrage, where companies leverage distinctions in national regulations to their advantage. To address these challenges, international coordination is becoming increasingly essential. Initiatives like the Financial Action Task Force (‘FATF’) guidelines aim to standardize regulations and combat financial crimes on a global scale.

In the United States (‘US’), regulatory bodies under the previous administration intensified enforcement activities, particularly focusing on classifying certain cryptocurrencies as securities. This approach subjected them to traditional financial regulatory requirements, sparking debates over definitions and the need for clearer

regulations. The new administration has adopted a different approach, aiming to develop a framework that fosters innovation while ensuring effective regulation. This includes considering the establishment of a national crypto reserve, which could promote stability and confidence in the market.

Meanwhile, the European Union (‘EU’) has advanced its Markets in Crypto-Assets (‘MiCA’) regulation, which aims to create a comprehensive framework for the crypto industry across member states. MiCA seeks to standardize rules, enhance consumer protection, and ensure market integrity, although national interpretations may vary. This effort reflects a broader trend towards creating robust regulatory frameworks that protect investors while encouraging innovation.

In Asia, regulatory approaches to the crypto industry vary significantly. Japan and Singapore have been supportive in implementing regulations that promote growth while ensuring compliance with international standards. Japan has established a structured system recognizing cryptocurrencies as legal property, while Singapore's regulatory framework is designed to be crypto-friendly, encouraging innovation. In contrast, China maintains strict controls, banning crypto trading and mining activities. For crypto exchanges, complying with local regulations is essential. It builds trust, protects investments, and contributes to the overall health of the crypto ecosystem. Exchanges that adhere to regulations are seen as more credible, and clear regulations provide a defined pathway to compliance, enhancing user trust. Crypto exchanges need to be strategic by implementing robust Know Your Customer (‘KYC’) and Anti-Money Laundering (‘AML’) measures, leveraging technology for compliance, and educating users about regulatory changes.

Navigating these challenges requires a strategic approach that balances innovation with compliance. As the crypto market continues to evolve, regulators worldwide are shifting from passive observation to proactive measures to ensure financial stability and consumer protection. The rapid growth of DeFi (‘Decentralized Finance’) and new cryptocurrency tokens is challenging traditional regulations. The global nature of the crypto industry adds complexity. Companies often operate in multiple countries without a physical base, leading to potential loopholes. To tackle these issues, international cooperation is essential, with efforts like the FATF working to create consistent rules and fight financial crimes worldwide.

Different regions are handling these challenges in various ways. In the U.S., regulators are focusing on clearer rules and guidelines. The EU's MiCA regulation aims to create a unified framework to protect consumers and ensure market integrity. In Asia, countries like Japan and Singapore have supportive regulations that encourage growth while meeting international standards. For crypto exchanges, local laws are crucial for building trust and safeguarding investments. By having strong KYC and AML compliance programs, exchanges can boost user confidence and support the crypto ecosystem. Embracing international cooperation and working towards standardized

regulatory frameworks will be critical in enhancing market integrity, protecting consumers, and promoting transparency in the digital asset era.

As global regulators strengthen efforts to enforce compliance and safeguard investors, the crypto industry must remain active and responsive to these developments.

ICC FraudNet
Global Annual Report 2025

Panamanian Public Order and its Impact on the Recognition and Enforcement of Foreign Judgments

**DONALD ANDERSSON SÁEZ
SAMANIEGO**



Panamanian Public Order and its Impact on the Recognition and Enforcement of Foreign Judgments

Donald Andersson Saez Samaniego
MDU LEGAL

Introduction

In this paper, the author addresses the importance of the notion of "public order" and its impact on the processes of "*exequatur*" or recognition and enforcement of foreign judgments, heard before the Fourth Chamber of General Affairs of the Supreme Court of Justice of the Republic of Panama. He also highlights how disregard for the principle of non-discrimination, violations of due process and the right to defense, as well as the usurpation of the exclusive jurisdiction of Panamanian courts, can prevent the recognition and enforcement of a foreign judgment in Panamanian jurisdiction.

Requirements to recognize and enforce foreign judgments ¹:

The recognition and enforcement of foreign judgments in the Republic of Panama are possible through the *exequatur process* and are heard before the Fourth Chamber of General Affairs of the Supreme Court of Justice. We have previously discussed the requirements for an *exequatur claim* to be admissible in Panama. For this purpose, the international treaties in force between the countries involved must be observed, and

¹ If you want to know more about the requirements for the recognition of Requirements to recognize and enforce foreign judgments, you might consult the article "*Enforcement of foreign judgments in Panama*", also written by the author, and published in the Global Annual Report 2024 – ICC FraudNet : <https://iccfraudnet.org/wp-content/uploads/2024/08/ICC-FraudNet-2024-Global-Annual-Report.pdf> [accessed April 03, 2025].

in their absence, article 1419 of the Panamanian Judicial Code,² in conjunction with Articles 155 and 156 of the Panamanian Code of Private International Law (Law No. 61 of October 8, 2015)³. These rules essentially establish the requirements for recognizing and enforcing a foreign judgment in Panamanian territory, which include:

*“... 1. That the judgment has been issued as a result of the exercise of a personal claim, except as specifically provided by law in matters of successions opened in foreign countries; 2. That it has not been issued in absentia, meaning, for the purposes of this article, the case in which the claim has not been personally notified to the defendant, having been ordered by the court of the case, unless the defaulting defendant requests execution; 3. That the **obligation** for the fulfillment of which the procedure has been carried out **is lawful in Panama**; and 4. The copy of the judgment must be authentic. A judgment is understood to be the decision that resolves the claim ...”* (Italics and emphasis added).

For the purposes of this paper, we are interested in addressing requirement number three in more depth and highlighting some hypothetical examples in which a judgment would not be lawful in Panama, making its recognition and enforcement impossible.

Panamanian Public Order and its impact on the recognition and enforcement of foreign judgments:

Regarding requirement number three, the concept of "Public Order" takes on special relevance, and in this regard, it is necessary to introduce its meaning. The Panamanian Code of Private International Law defines it in Article 160 as:

*32. Public order or Panamanian public order. " A set of **mandatory rules** of Panamanian law that the parties **cannot disregard**." (Emphasis added).*

In other words, Public Order refers to the set of basic rules that the parties (people) and, in addition, the Panamanian State as guarantor of the application of the laws, cannot ignore under any circumstances, since they are mandatory, so their application cannot be ignored.

The Panamanian Code of Private International Law establishes that foreign acts or laws will not be recognized in whole or in part when their application in Panama violates public order:

Article 7. The legal effects of a foreign act or law shall not be recognized, in whole or in part, when its application violates or infringes international public order.

² The Judicial Code of Panama can be consulted at: <https://vlex.com.pa/vid/codigo-judicial-58511374>

³ Official Gazette of Panama 27885-A of October 8, 2015, available at: https://www.gacetaoficial.gob.pa/pdfTemp/27885_A/GacetaNo_27885a_20151008.pdf

Any foreign law not applied shall be replaced by domestic law. (Emphasis and italics added.)

The legal provisions cited summarize the importance of Panamanian public order, while, together with Article 37 of the same Code, they address the legal effects that public order would have in the face of a foreign act or judgment that is contrary to the basic and elementary principles and whose recognition and enforcement is attempted in Panama:

“Article 37. Foreign law shall not be applied when it is contrary to Panamanian public order or when the application or invocation of foreign law has constituted a violation of the law that should have regulated the act or legal relationship under examination.

The courts shall not enforce judicial or administrative decisions declaring any rights without confirming that the decisions issued in a foreign country were issued by a competent authority, in accordance with applicable foreign domestic law, and that they were not issued in absentia.” (Emphasis and italics added.)

Principle of non-discrimination:

A basic constitutional principle and right that constitutes the so-called "Public Order" is the right to non-discrimination. It is a recognized minimum right that does not exclude any person, whether Panamanian or foreign. In this regard, it is important to mention that if a person is sanctioned by a civil or commercial court ruling solely for reasons of race, gender, religious orientation, or similar discrimination that demonstrates unlawful discrimination, said ruling could be invalid in Panama, rendering it null and void. The principle of non-discrimination is part of public order and is established in Article 19 of the Panamanian Constitution ⁴.

Violation of due process and right to defense:

Due process is part of the Panamanian constitutional order and is found in Article 32 of the Political Constitution of Panama. This establishes the right to be judged "in accordance with legal procedures." This means that, in order for a judgment to be recognized or enforced in Panama, the party against whom the judgment is sought to be enforced must have been guaranteed certain rights, such as: the right to be represented by counsel; the right to present evidence; the right to use all available legal remedies within the timeframes and in the manner determined by applicable law, among others.

⁴ Political Constitution of Panama can be consulted at: <https://ministeriopublico.gob.pa/wp-content/uploads/2016/09/constitucion-politica-con-indice-analitico.pdf> (accessed 1 July 2025)

Violation of the exclusive jurisdiction of Panamanian courts:

For reasons of sovereignty and national interest, Panama reserves exclusive jurisdiction to hear certain matters, such as the dissolution or liquidation of legal entities incorporated in Panama;⁵ claims arising from representation and franchise agreements when these are executed in Panama;⁶ claims arising from real estate located in Panama,⁷ among others. All of the aforementioned scenarios, where a foreign court usurps the exclusive jurisdiction of Panamanian courts, will result in the non-recognition or enforcement in Panama of any judgment issued by that court.

Conclusion

Public order embodies the fundamental principles, rules, and rights that cannot be ignored by either the individual or the State. These are mandatory and imperative, and no foreign act, judgment, or law may reduce or contravene them; otherwise, their effects in Panama are considered null and void.

When filing legal proceedings abroad that may have an impact or whose recognition is subsequently sought in Panama, it is important to verify and conduct a preventive examination of the potential validity of the judgment resulting from said proceedings, in order to avoid unnecessary loss of time and legal expenses.

⁵ Code of Private International Law, article 24. Available at: Official Gazette of Panama 27885-A of October 8, 2015:
https://www.gacetaoficial.gob.pa/pdfTemp/27885_A/GacetaNo_27885a_20151008.pdf (accessed 8 July 2025)

⁶ Ib. Article 83.

⁷ Ib. Article 156.



ICC FraudNet
Global Annual Report 2025

Part III: Asset Recovery Investigations: Criminal, Civil and Technological Perspectives



ICC FraudNet
Global Annual Report 2025

Dealing with the Challenge of Encrypted Messaging Apps

**MARTIN KENNEY AND
HARLEY THOMAS**

iccfraudnet.org

ICC |  **FraudNet**



Dealing with the Challenge of Encrypted Messaging Apps

Martin Kenney & Harley Thomas
MKS Law

Introduction

Success in asset recovery and criminal accountability will increasingly hinge on adaptive strategies that mirror fraudsters' agility, harnessing technology and international cooperation to overcome substantial evidentiary and jurisdictional barriers.

The revelation that members of the US government shared extremely sensitive military operational information via the Signal messaging app has brought into close focus just how common encrypted messaging has become.¹

Journalists, politicians and, of course, the criminal fraternity have all turned to encrypted messaging platforms. These have unfortunately become integral tools in global fraud schemes, too, posing significant challenges for asset recovery professionals. While platforms like Signal, Telegram and WhatsApp provide valuable privacy protections for legitimate users, they have simultaneously evolved into a critical infrastructure for orchestrating and concealing sophisticated financial crimes.

Fraudsters leverage these encrypted architectures with their decentralised communication and limited metadata retention, to perpetrate cryptocurrency scams,

¹ See: <https://www.nytimes.com/2025/04/20/us/politics/hegseth-yemen-attack-second-signal-chat.html> (accessed 15 June 2025)

investment fraud and advanced asset concealment operations, complicating cross-border investigations and recovery efforts.

Large-scale organised fraud groups frequently take advantage of Telegram's client-side open-source structure, for example. These criminal enterprises exploit the app's expansive private groups, promoting fraudulent investment opportunities and directing victims toward decentralised cryptocurrency exchanges or peer-to-peer transactions.

Conversely, WhatsApp is commonly utilised for intensive, targeted engagement through one-to-one interactions, notably in so-called "pig butchering" (romance) schemes. Victims are meticulously groomed over extended periods, fostering trust and deepening deception, before being persuaded to part with their funds.

Law enforcement agencies face substantial difficulties when securing crucial evidence from any of these encrypted mobile platforms. Investigators typically begin by attempting to access encrypted data directly from seized mobile devices. Yet the challenges posed by device encryption, local storage permissions and auto-deletion features often hinder forensic retrieval.

In the UK, law enforcement can legally access communications through device seizures under existing legislation, via the Police & Criminal Evidence Act 1984, the Investigatory Powers Act 2016 and the Regulation of Investigatory Powers Act 2000. However, practical retrieval is often limited by the technical nature of the layered encryption and remotely stored electronic data ('RSED').

Barriers and hurdles

Legal and evidentiary hurdles compound these technical challenges. There are severe obstacles for investigators dealing with Telegram, for example, while WhatsApp operates under US jurisdiction and for UK investigators, at least, there is the slow pace of mutual legal assistance treaty ('MLAT') processes to navigate.

Consequently, evidence admissibility is frequently contested. For instance, the European Union's General Data Protection Regulation ('GDPR') imposes strict rules on data access and transfer, which can delay or hinder cross-border access to encrypted communications.

Forensic strategies now include a blend of blockchain analytics, open-source intelligence ('OSINT'), and metadata triangulation to mitigate these barriers. Platforms such as Chainalysis, TRM Labs and Elliptic facilitate tracing assets across crypto wallets. Investigators routinely combine these analytical tools with linguistic analysis and device imaging.

This allows investigators to construct models revealing links between suspects across platforms, transactions and communication trails. Metadata such as IP logs, device

identifiers and timestamps also provide essential leads even when message content remains inaccessible. Yet criminals are sophisticated too and these specialist companies have varying capabilities and experience when faced with these complex tasks.

Breakthroughs

Recent legal innovations reflect a growing awareness of the need for adaptive procedural strategies. Asset recovery litigators increasingly pursue worldwide freezing orders to halt asset dissipation, targeting exchanges and digital asset custodians that are identified via forensic tracing.

Composite disclosure orders, merging Norwich Pharmacal Orders with international cooperation instruments (such as letters of request/letters rogatory, or Hague Convention requests), enable simultaneous cross-jurisdictional disclosures, significantly enhancing this process.

Additionally, disclosure requests directed at third-party entities, including internet service providers, virtual private network providers, hosting services and payment processors, play a critical role in uncovering crucial metadata.

Courts in offshore jurisdictions, notably the British Virgin Islands and Cayman Islands, have shown growing flexibility in adapting proprietary injunction principles specifically for digital asset recovery. However, compliance with digital sovereignty laws, such as GDPR data protection protocols, means careful coordination is necessary in order to prevent procedural complications or delays.

This is a rapidly evolving landscape. There are procedural innovations emerging, such as the ability to serve legal notices via digital NFTs (non-fungible tokens), as well as the growth of technologies such as smart contracts, which automate the actions required in blockchain transactions. These align potential remedies to the operational realities of digital-native criminal environments.

UK law enforcement agencies also actively collaborate with their international counterparts in this arena, including EC3 (Europol Cybercrime Centre) and JCAT (Joint Cybercrime Action Task Force). Such intelligence sharing, and the use of joint investigative task forces and parallel civil and criminal proceedings, increases the effectiveness of asset recovery efforts.

UK enforcement developments and the EncroChat precedent

Another key development in the fight against encrypted criminal communications, from a UK perspective, has been the relatively recent success of the National Crime Agency ('NCA').

In 2020, working with French and Dutch authorities under Eurojust and Europol coordination, the NCA gained covert access to millions of messages sent via EncroChat, an encrypted phone service used almost exclusively by organised crime networks.

This led to Operation Venetic and thousands of subsequent arrests, as well as seizure of assets and prosecutions. It is deemed a landmark success in this space. The operation demonstrated not only the value of technological infiltration, but also the critical role that international cooperation plays in piercing the veil of encrypted messaging systems.

The UK courts upheld the admissibility of intercepted EncroChat messages, even where live intercepts would typically breach domestic law under the Investigatory Powers Act 2016. This precedent has instigated a broader legal debate around admissibility of digital evidence, interception standards, and the balance between privacy rights and public interest in the digital age.

The EncroChat litigation has underscored the possibility of using intercepted communications as primary evidence in serious and complex fraud and money laundering cases, a key development in prosecutorial strategies.

This success has emboldened UK law enforcement and intelligence agencies to invest further in offensive cyber capabilities and infiltration techniques. The NCA's recent launch of a National Security and Cyber Crime Unit ('NSCCU'), detailed in its 2025 strategy, confirms a shift toward more proactive, intelligence-led operations, particularly targeting crypto-enabled organised crime. The NSCCU's mission includes penetrating encrypted messaging ecosystems, deploying lawful hacking capabilities, and enhancing data acquisition through international alliances.

Notably, UK authorities are increasingly deploying civil recovery powers under the Proceeds of Crime Act 2002 ('POCA') in parallel with criminal investigations. These powers allow the freezing and forfeiture of assets even where criminal convictions are not secured, a vital tool when prosecutorial evidence remains locked behind encrypted systems or foreign legal barriers. Civil asset recovery claims are often paired with disclosure applications and third-party subpoenas to exchanges, custodians, and service providers who facilitate or unknowingly host criminal activity.

The EncroChat example, combined with the legal flexibility of civil recovery mechanisms and the rising strategic importance of public-private partnerships, points to a future in which UK enforcement agencies take a more active role in combating fraud via encrypted platforms.

These developments also reflect growing judicial comfort with novel evidentiary sources, technical expert input and hybrid legal proceedings. As encrypted messaging

usage proliferates among fraudsters, so too must the legal and technical agility of those charged with pursuing them.

Conclusion

In conclusion, addressing the misuse of encrypted messaging platforms in global fraud schemes demands multi-jurisdictional collaboration, sophisticated technological fluency and continuous procedural innovation.

Success in asset recovery and criminal accountability will increasingly hinge on adaptive strategies that mirror fraudsters' agility, harnessing technology and international cooperation to overcome substantial evidentiary and jurisdictional barriers.

Proactive engagement between law enforcement agencies, regulatory bodies and legal professionals will further strengthen these collaborative frameworks.

ICC FraudNet
Global Annual Report 2025

Large Language Models ('LLMs') as Translators of Investigative Intuition

KRISTIN DEL ROSSO



Large Language Models (‘LLMs’) as Translators of Investigative Intuition

Kristin Del Rosso
DevSec

Abstract

This paper examines how Large Language Models (‘LLMs’) provide dramatic operational uplift for complex fraud investigations by augmenting two key areas – investigator intuition and data discovery. Traditional investigation tools struggle with unstructured data and rely heavily on static queries. LLMs allow investigators to produce structured outputs from unstructured data and dynamically generate queries based on the user's intent - even a relatively simple pipeline can increase the effectiveness of analysis at scale. To demonstrate this emerging capability, we assess a case study from a recent DevSec investigation involving the identification and extraction of cryptowallets from years of chat logs. Our paper describes an iterative two-phase workflow of dynamic pattern generation and context validation – enabling rapid identification of relevant evidence and the context in which that evidence exists. We detail a modular architecture separating reasoning from retrieval, which ensures auditability, and outlines best practices for integrating LLMs into investigative workflows. The result is faster, more accurate discovery and a blueprint for scalable fraud detection.

Introduction

Modern fraud investigations confront unprecedented volumes of data – including millions of documents, chat logs, emails, and individual files. Investigators may not know precisely what they are looking for in advance, but they do have a general sense

of what might be relevant, such as references to illicit transactions, complex cryptocurrency wallet addresses, or subtle patterns of suspicious behavior. Once encountered, these elements immediately stand out to experienced investigators as critical pieces of evidence and can be leveraged as search patterns within a large data corpus to generate investigative leads.

Conventional investigative tools rely on rigid keywords or Boolean logic, demanding exact terms and struggling with variations in context and format. This generates a significant amount of false positives when targets are poorly defined and this presents a bottleneck on investigation resources. Our approach leverages an LLM to serve as an interpretation layer between the investigator and the tool. This transforms investigative intuition into precise, context-aware queries that rapidly surface actionable insights.

Case Study: Crypto Wallet Discovery in Cybercrime Chat Logs

LLMs bridge the gap between intuitive investigative questions and concrete data retrieval. DevSec was recently engaged to support a cybercrime investigation, with the goal of identifying cryptocurrency wallets buried within years of unstructured forum messages – without knowing which blockchain or address format to target. Traditional tooling offered no straightforward solution aside from requiring the experts to read through the forum messages to identify wallets and individually write structured queries.

Instead, investigators leveraged an LLM to generate a wide variety of potential Regular Expression (“RegEx”) patterns for multiple wallet formats (i.e. Bitcoin, Ethereum and others). This allowed the team to test a wide variety of queries and extract candidate strings from the text. The team then used an LLM as a reasoning and classification tool to validate each candidate in the context of the initial chat log and with custom instructions for what the investigation was targeting. This filtered out a significant amount of false positives and associated confirmed wallets with their associated user handles. What would have taken weeks of manual review was completed in just a few hours, yielding a concise list of high-confidence wallet IDs for follow-up.

With a simple natural-language instruction – “Identify cryptocurrency wallet addresses in the following chat logs” – an LLM reasoned about the patterns and context required to locate relevant evidence. In this role, the LLM functioned as an intelligent intermediary that dynamically constructed search logic, orchestrated tool invocations, and dramatically accelerated discovery.

Iterative Reasoning Workflow

Behind the scenes, the LLM followed a transparent chain-of-thought, alternating between reasoning and tool calls. A simplified excerpt of its internal log demonstrates this audit trail:

1. Reasoning: Determine relevant wallet formats given the investigator's prompt.
2. Tool Call: Use a RegEx generator to generate patterns.
3. Reasoning: Apply patterns to extract candidates, then validate each match in context.
4. Tool Call: Use a pattern matcher to extract candidates.
5. Tool Call: Use context validation to filter on high confidence results.

System Architecture: Separation of Reasoning and Retrieval

The system architecture decouples reasoning (LLM) from retrieval (specialized tools and secure data storage). A lightweight router parses natural-language queries and forwards them to the LLM, which orchestrates tool calls against a controlled data layer. All queries, tool invocations and results are logged to create an auditable chain of custody – minimizing hallucination risk and ensuring transparency.

Practical Implications and Best Practices

Effective LLM integration demands human oversight, iterative prompt refinement and rigorous validation of outputs. Organizations should adopt an extraction and validation workflow, maintain exhaustive logs of model reasoning, and continuously benchmark performance. This approach reduces time to insight, enhances accuracy and frees investigators to focus on strategic analysis rather than routine data retrieval.

Future Outlook

As data volumes grow and fraud schemes evolve, LLM-powered discovery will become indispensable. Future enhancements may include multilingual processing, cross-dataset linkage, and predictive relationship mapping. By converting investigative intuition into actionable leads at unprecedented speed, LLMs redefine the frontier of complex fraud investigations. Additionally, LLM-assisted discovery does not replace human expertise – it amplifies it. By translating vague investigative instincts into precise evidence with full auditability, LLMs empower investigators to move swiftly from intuition to insight, reshaping the fight against financial crime.

The background of the cover is a collage of various US dollar bills, including one, five, and ten dollar bills, arranged in a dynamic, overlapping fashion. A large, semi-transparent maroon rectangle covers the upper right portion of the image, serving as a backdrop for the title and authors' names.

ICC FraudNet
Global Annual Report 2025

Assessing the Suitability of Different Cash Tracing Methodologies

**RICHARD FREEMAN,
MARCELA PITTELLI AND
TREVOR WILES**

iccfraudnet.org





Assessing the Suitability of Different Cash Tracing Methodologies

Richard Freeman, Marcela Pittelli, and Trevor Wiles
Forensic Risk Alliance ('FRA')

There are many reasons why funds must be traced to their end destination; asset tracing exercises are a key one, among others such as fraud investigations, disputes, and Anti-Terrorism Act claims. Cash tracing is a forensic accounting technique used to trace the flow of funds through a set of bank statements or financial accounting records to identify the beneficiaries of certain funds.

Cash tracing is made more difficult when the specific funds to be traced are comingled in a bank account with other funds from different sources. Further complications arise if the funds are transferred between multiple bank accounts and different currencies, resulting in various different threads to be followed. All these complications can make it a very time consuming exercise to trace the beneficiaries of the funds you are interested in. Notwithstanding these challenges, forensic accountants have typically relied on four commonly used tracing methods:

1. First In, First Out ('FIFO');
2. Last In, First Out ('LIFO');
3. Lowest Intermediate Balance Rule ('LIBR');
4. Pro Rata Tracing.

Each of these methodologies is based on the premise that money is fungible and provides a way to trace specific transfers to the ultimate beneficiary in an equitable manner. The appropriate methodology varies according to the specific circumstances of each case, and frequently different methodologies are used to identify the most suitable one. This article discusses each of these methodologies and their practical applications and limitations.

1. First In, First Out ('FIFO') Tracing

The FIFO method assumes that the first money deposited into an account is the first to be withdrawn. Thus, in circumstances where the funds to be traced ('the subject funds') are deposited into an account with an existing balance, the existing balance must be expended first, by subsequent withdrawals. Once the existing balance is expended, the subject funds can be traced to withdrawals from the account. Exhibit 1 below shows a hypothetical tracing exercise using this methodology.

Exhibit 1

Date	Transaction	Account balance	Opening balance	Balance of subject funds	Other deposits
March 1	Opening balance of \$200	200	200	0	0
March 2	Deposit of \$500 subject funds	700	200	500	0
March 3	Withdrawal of \$100	600	100	500	0
March 4	Deposit of \$200	800	100	500	200
March 5	Withdrawal of \$400	400	0	200	200
March 6	Withdrawal of \$100	300	0	100	200
March 7	Deposit of \$300	600	0	100	500
March 8	Withdrawal of \$50	550	0	50	500
March 9	Withdrawal of \$350	200	0	0	200

Using FIFO, the opening balance is expended first, leaving subsequent balances untouched until the subject funds are expended. Therefore, the traceable payments relevant to the \$500 subject funds are the withdrawals made on March 5, March 6, March 8 and March 9 (shown in yellow).

2. Last In, First Out ('LIFO') Tracing

Conversely, the LIFO method assumes that the most recent deposit into an account is the first to be withdrawn. If there are deposits into the account after the subject funds have been received, those deposits must be expended first before the subject funds can be traced to withdrawals. This method is generally preferable when the opening balance of an account should be retained and the subject funds should be traced to the next subsequent withdrawal, rather than expending the opening balance of funds first. Exhibit 2 below shows the result of this methodology when applied to the same hypothetical factual pattern as Exhibit 1.

Exhibit 2

Date	Transaction	Account balance	Opening balance	Balance of subject funds	Other deposits
March 1	Opening balance of \$200	200	200	0	0
March 2	Deposit of \$500 subject funds	700	200	500	0
March 3	Withdrawal of \$100	600	200	400	0
March 4	Deposit of \$200	800	200	400	200
March 5	Withdrawal of \$400	400	200	200	0
March 6	Withdrawal of \$100	300	200	100	0
March 7	Deposit of \$300	600	200	100	300
March 8	Withdrawal of \$50	550	200	100	250
March 9	Withdrawal of \$350	200	200	0	0

Using LIFO, the withdrawal on March 3 immediately after the deposit of the subject funds is traced to the subject funds. The deposits of other funds on March 4 and March 7 each have to be traced before the tracing of the subject funds can continue. Therefore, the withdrawals relevant to the \$500 subject funds are the withdrawals made on March 3, March 5, March 6 and March 9 (shown in yellow).

3. Lowest Intermediate Balance Rule ('LIBR')

The LIBR methodology assumes that any funds received either before or after the subject transfers must be expended first, before any withdrawals can be attributed to the subject funds. LIBR therefore assumes that the subject funds are the last to leave the account. The LIBR methodology is sometimes used in situations where funds received subject to a fraud are comingled with otherwise legitimate funds, because this methodology "preserves" any balance remaining in the bank account for the 'benefit' of defrauded victims (where the legal action is aimed at returning funds to the plaintiffs). Exhibit 3 shows the result of applying this methodology to the same hypothetical factual pattern considered previously.

Exhibit 3

Date	Transaction	Account balance	Opening balance	Balance of subject funds	Other deposits
Mar-01	Opening balance of \$200	200	200	-	-
Mar-02	Deposit of \$500 subject funds	700	200	500	-
Mar-03	Withdrawal of \$100	600	100	500	-
Mar-04	Deposit of \$200	800	100	500	200
Mar-05	Withdrawal of \$400	400	-	400	-
Mar-06	Withdrawal of \$100	300	-	300	-
Mar-07	Deposit of \$300	600	-	300	300
Mar-08	Withdrawal of \$50	550	-	300	250
Mar-09	Withdrawal of \$350	200	-	200	-

Using LIBR, the subject funds are considered the last to leave the account. Therefore, the withdrawals relevant to the \$500 subject funds are those made on March 5, March 6 and March 9 (shown in yellow). In the example above, \$200 of the subject funds remain in the account at the end of the review period (also the value of funds remaining in the bank account).

4. Pro Rata Tracing

Pro Rata Tracing assumes that all deposits in an account contribute proportionally to all subsequent withdrawals. Unlike the previous methodologies, which prioritize certain transactions over others, pro rata tracing distributes the impact of withdrawals across all deposits based on their relative sizes. The Pro Rata method is suitable in cases where there is no evidence to distinguish between the subject funds and all other funds deposited in the account. This method is often preferred when there are several similar claims for restitution over the recovered amounts (i.e., Ponzi scheme victims would be compensated in proportion to their net deposits into the scheme). However, under the Pro Rata methodology, funds will remain subject to allocation until the bank account reaches a balance of zero, which may take a long time, if it ever happens. If the entity's bank accounts in question are still open, so long as the balances never reached zero, then historic funds transferred into those accounts would still be linked to transactions occurring today in increasingly diminishing amounts, as shown in Exhibit 4 below.

Exhibit 4

Date	Transaction	Account balance	Opening balance	Balance of subject funds	Other deposits
Mar-01	Opening balance of \$200	200	200	-	-
Mar-02	Deposit of \$500 subject funds	700	200	500	-
Mar-03	Withdrawal of \$100	600	171	429	-
Mar-04	Deposit of \$200	800	171	429	200
Mar-05	Withdrawal of \$400	400	86	214	100
Mar-06	Withdrawal of \$100	300	64	161	75
Mar-07	Deposit of \$300	600	64	161	375
Mar-08	Withdrawal of \$50	550	59	147	344
Mar-09	Withdrawal of \$350	200	21	54	125

Using the Pro Rata method, as long as there are funds in the account after the subject funds were deposited, all subsequent withdrawals will include a percentage of the subject funds. Therefore, the withdrawals relevant to the \$500 subject funds are those made on March 3, March 5, March 6, March 8, and March 9 (shown in yellow). In the example above, \$54 of the subject funds remain in the account at the last date. A balance of the subject funds will remain in the account until the account balance reaches zero.

Other complications

It is important to apply the methodologies to standardized data sets, which may not be readily available. Bank statements are the preferable data source but often do not include details on the beneficiary of transactions. Even where bank statements are available and complete, they may be in different formats (i.e., excel statements are easier to review than poorly scanned ones) and require significant standardization before the analysis can begin. Where bank statements do not include beneficiary details or are simply unavailable, transactions may be traced via the general ledger, which often needs to be joined to other accounting tables to identify the counterparty and value date of each transaction. This requires input from data analytics specialists.

Conclusion: choosing the appropriate methodology

The methodologies of FIFO, LIFO, LIBR, and Pro Rata tracing each have theoretical justifications and practical applications suited to different cases. The method used depends on the circumstances and claimants will likely use the one best suited to their claim. The results of each methodology ultimately depend on the fact patterns (i.e., the chronology of the subject funds versus other deposits and withdrawals). The choice of one methodology over the other needs to be justified by the underlying facts of the matter, and often the exercise will be performed under different methodologies to show the appropriateness of one over another. Experience shows that courts will allow any method to be used if it is argued effectively and is equitable.



ICC FraudNet
Global Annual Report 2025

Asset Recovery in Spain: Civil and Criminal Law Mechanisms

**FABIO VIRZI AND OSCAR
MORALES**

iccfraudnet.org

ICC |  **FraudNet**



Asset Recovery in Spain: Civil and Criminal Law Mechanisms

Fabio Virzi, ECIJA

Oscar Morales Ph.D., Cases and Lacambra

This article analyses the main legal mechanisms available within the Spanish legal system for pursuing the assets of debtors, both through civil and criminal law pathways.

From a civil law perspective, we examine judicial actions for asset recovery, detailing procedures available according to the type and amount of debt, including ordinary and summary proceedings, the order for payment, and bill of exchange procedures. Special emphasis is placed on the processes for recognizing and enforcing foreign judgments through exequatur, the adoption of precautionary measures to prevent asset dissipation, and specific liability actions against corporate directors, including the piercing of the corporate veil doctrine.

In the criminal law context, we discuss precautionary measures applicable to criminal proceedings, asset confiscation procedures, enforcement of criminal judgments, and the specific offence of fraudulent conveyance aimed at preventing asset concealment. Particular attention is given to the conditions required to adopt these measures and their procedural implications, highlighting differences from civil proceedings.

Overall, the article emphasizes the strategic importance of understanding these tools for effective asset recovery in Spain, especially within an international context characterized by debtor asset concealment and jurisdictional complexities.

As a consequence of globalisation, it is increasingly common for a creditor to hold a credit right against a debtor whose assets are located in another jurisdiction. This

situation compels the creditor to deploy transnational recovery strategies, facing challenges arising from the diversity of legal systems and the potential manoeuvres of the debtor to conceal or transfer their assets.

To mitigate the risk of asset depletion and maximise the chances of credit recovery, it is essential for the creditor to understand the legal framework applicable in the country where the debtor's assets are located. This article analyses the main mechanisms available in the Spanish legal system for asset recovery from both civil and criminal law perspectives.

1. Mechanisms for Asset Recovery from a Civil Law Perspective

Judicial Actions for Asset Recovery

The Spanish legal system provides various judicial avenues for asset recovery, depending on the nature and amount of the claimed credit. Traditionally, monetary claims were processed through ordinary proceedings if the amount exceeded €6,000 and through summary proceedings if it was lower. However, following the reform of the Spanish Civil Procedure Act, claims are now handled through ordinary proceedings when the amount exceeds €15,000.

Summary proceedings are faster, allowing the judge to issue a ruling without a hearing if the parties do not deem it necessary. In contrast, ordinary proceedings involve a preliminary hearing to determine disputed facts and propose evidence, with the possibility of a subsequent trial if witness evidence is required.

There are also specific procedures for claims based on documents with particular characteristics. The order for payment procedure allows creditors to claim liquid, certain, due, and payable debts, provided they are evidenced by documents signed by the debtor, invoices, delivery notes, or certifications reflecting the commercial relationship. The main advantage of this procedure is its speed, as the court requires the debtor to pay without the need for a formal lawsuit. However, if the debtor contests the claim, the process is transformed into a summary or ordinary trial, depending on the amount involved.

Another option is the bill of exchange proceeding, applicable when the debt is documented in negotiable instruments such as bills of exchange, cheques, or promissory notes. This mechanism allows the creditor to obtain an immediate payment order and, in case of non-payment, proceed with the attachment of the debtor's assets. Once a judgment (in the case of ordinary or summary proceedings) or a ruling declaring the enforcement of the debt (in the case of the order for payment procedure) has been issued, if the debtor fails to voluntarily satisfy the debt, the creditor may request the enforcement of the relevant resolution by initiating enforcement proceedings. In this context, the creditor may ask the judge to investigate and determine the debtor's assets,

as outside judicial proceedings, the only means of obtaining such information in Spain is through public registers, such as the Land Registry.

Recognition and Enforcement of Foreign Judgments

In an international context, asset recovery may depend on the recognition and enforcement of foreign judgments. In Spain, this procedure is governed by *exequatur*, a judicial process that verifies the validity of the foreign judgment.

The treatment varies depending on the origin of the judgment. If it comes from an EU Member State, its recognition is automatic under Regulation (EU) 1215/2012 (Brussels I Bis). For judgments issued in Norway, Iceland, or Switzerland, the Lugano Convention of 2007 applies. For judgments from non-EU countries, international conventions or bilateral agreements between Spain and the country of origin may be applicable. In the absence of an applicable treaty, the Spanish Law on International Legal Cooperation is followed.

If the ruling is not a judicial judgment but an arbitral award, the *exequatur* procedure is also required, but in this case, the applicable regulation is the 1958 New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards.

As in the enforcement of domestic judgments, in the enforcement of foreign rulings, the creditor may request the court to conduct an asset investigation into the debtor, in order to locate assets in Spanish territory that may be used to satisfy the recognised judgment.

Precautionary Measures to Prevent Asset Dissipation

One of the main risks in asset recovery is the possibility that the debtor may dissipate their assets before the creditor can enforce their claim. To prevent this, the Spanish legal system allows the adoption of precautionary measures within judicial proceedings, both in monetary claims and in the recognition and enforcement of foreign judgments.

Precautionary measures may be requested either simultaneously with the filing of the lawsuit or prior to its submission, where urgent circumstances exist. In the latter case, if the measure is granted, the claimant must file the lawsuit within a maximum period of 20 days.

For the court to grant a precautionary measure, the following requirements must be met:

1. **Appearance of good right (*fumus boni iuris*)** – The applicant must preliminarily demonstrate that their claim has sufficient legal grounds.

2. **Risk of frustration of enforcement (*periculum in mora*)** – It must be justified that, if the measure is not immediately adopted, the future enforcement of the judgment could be compromised by actions of the debtor, such as asset sales or concealment.
3. **Proportionality and security** – The court will assess whether the requested measure is proportional to the harm sought to be prevented. Additionally, the applicant must provide financial security to compensate for any potential damages to the debtor if the precautionary measure is ultimately revoked.

Furthermore, precautionary measures may be requested *inaudita parte*, that is, without prior notice to the debtor, when there is a clear risk that prior knowledge could compromise the effectiveness of the measure, such as in cases of asset concealment or dissipation.

Liability Actions Against Directors and Piercing the Corporate Veil

When the debtor operates through a corporate entity, mechanisms exist to allow direct claims against its directors. The individual liability action enables the creditor to sue directors when their negligent or unlawful actions have directly caused damage. In cases of corporate insolvency, the action for liability for corporate debts may compel directors to be personally liable for the company's debts.

Additionally, if it is proven that the company has been fraudulently used as a vehicle to evade liabilities by its shareholders, the piercing of the corporate veil doctrine may be invoked, allowing creditors to hold shareholders directly liable with their personal assets.

These mechanisms are essential in scenarios where complex corporate structures are used to hinder debt enforcement and protect the assets of those ultimately responsible. Consequently, asset recovery in Spain from a civil law perspective provides multiple tools to protect creditors' interests, enabling the enforcement of judgments, the adoption of precautionary measures, and the liability of directors in cases where they have engaged in unlawful acts that have directly harmed the assets of the company's creditors. However, in certain situations the Spanish legal system also provides criminal law mechanisms that can reinforce the creditor's ability to recover assets.

Criminal law can be a crucial tool in cases where the debtor has engaged in illicit practices. The prosecution of these offences not only allows for criminal sanctions but may also facilitate the restitution of assets to the victim of the offence. The following section will examine the main criminal law mechanisms available in Spain for asset recovery in judicial proceedings.

2. Mechanisms for Asset Recovery from a Criminal Law Perspective.

Spanish Criminal Law provides three main avenues for asset recovery: (i) precautionary measures; (ii) confiscation; and (iii) enforcement of judgments. In addition, the measures outlined in this article are strengthened within the Spanish Criminal jurisdiction by the existence of a specific offence aimed at preventing asset concealment behaviors. A detailed explanation of these elements follows.

Precautionary Measures in Criminal Proceedings

In criminal proceedings, precautionary measures refer to court-ordered actions that affect the defendant's assets. These measures aim to secure potential financial liabilities that may arise from the defendant's criminal responsibility.

Precautionary measures encompass a broad scope, covering not only rulings specific to criminal proceedings — such as potential fines, asset confiscation, or court costs — but also civil liability arising from a criminal offence.

Regarding the specific precautionary measures that may be adopted for asset recovery within the scope of criminal proceedings, the current regulation provides for the following measures:

- a. Seizure of assets.
- b. Asset freeze.
- c. Financial security.
- d. Judicial intervention.
- e. Judicial management.
- f. Deposit of assets.
- g. Asset inventory.
- h. Suspension of shareholder agreements.
- i. Temporary closure of establishments.
- j. Temporary suspension of activity.
- k. Preventive notice of asset restriction.

The type of measures adopted to preserve the defendant's assets and ensure potential liability hinges on the prevailing circumstances. In this regard, certain measures may prove appropriate, while others may not. Assessing this matter requires observing specific principles, which will be analysed below.

The regulation of precautionary measures in Spanish Criminal Law draws subsidiarily on the provisions of Spanish Civil Procedure Code, pursuant to Articles 589 *et seq.* and 764 of the Spanish Criminal Procedure Code (hereinafter, 'SCPC'). Accordingly, compliance with the two previously analysed requirements becomes mandatory:

- (i) A *prima facie* case (“*fumus boni iuris*”), which, in criminal proceedings, directly relates to the existence and severity of reasonable suspicion of criminal conduct; and
- (ii) Risk of frustration of enforcement (“*periculum in mora*”), which implies that, if the Court does not order precautionary measures, the defendant’s assets may be concealed or transferred, undermining the effectiveness of a future judgment.

Nevertheless, a significant distinction exists compared to civil regulation, as criminal proceedings do not require financial security as a basis for ordering precautionary measures. This divergence arises from the principles of instrumentality and officiality, which govern criminal proceedings:

- (i) Pursuant to the principle of instrumentality, criminal proceedings pursue the prosecution and punishment of the most serious offences. Consequently, they are grounded in an inalienable general interest that cannot be conditioned upon the provision or absence of financial security.
- (ii) In adherence to the principle of officiality, state institutions — specifically the Public Prosecutor’s Office, Investigative Courts, and Trial Courts — bear the duty to eliminate any obstacle to the prosecution of criminal offences and the redress of their consequences.

Provided the aforementioned grounds are satisfied, precautionary measures may be adopted either *ex officio* by the Court or upon request by the parties at any stage of the criminal proceedings: (i) from the admission of the criminal complaint throughout the initial phase of the proceedings (the investigation stage); and (ii) through the judicial ruling that initiates the trial phase.

Any restriction of fundamental rights must be duly justified, as established by the Judgment of the Spanish Constitutional Court No. 62/1982, among many others. According to this ruling, the grounds for the restriction must be communicated to the affected party; otherwise, the right to due process would be violated. For this reason, Article 764 SCPC mandates that any precautionary measure must be adopted through a reasoned judicial decision.

Notwithstanding, an exception to the requirement of notifying the affected party of the grounds exists: Article 302 SCPC allows for the secrecy of the criminal proceedings to be ordered, either partially or fully, including from the defendant, with the sole exception of the Public Prosecutor.

In such cases, where secrecy has been duly ordered, neither the content nor the reasoning behind the judicial decision on precautionary measures shall be disclosed to the defendant, without this constituting a violation of the right to due process.

In addition to a reasoned judicial decision, other formal requirements apply to precautionary measures: the aforementioned Article 764 of the SCPC also mandates that precautionary measures must be formalized in a separate section of the proceedings. This provision recognizes precautionary measures as matters requiring autonomous treatment from the main procedure, while remaining inherently connected to it.

Confiscation of Assets

Confiscation of assets constitutes a **criminal sanction**, equivalent to a penalty, ordered by a Court. It entails the forfeiture of assets derived directly or indirectly from a criminal offence, those used in its commission, and any profits obtained from criminal activity.

While precautionary measures seek to preserve the defendant's assets to ensure the enforcement of potential criminal and civil liabilities, asset confiscation aims to prevent the use and enjoyment of illicitly obtained proceeds.

The principle underlying the institution of confiscation is that criminal offences must neither generate nor retain profits. This concept has extended beyond national legislation, influencing both European and International Law, reflecting a firm conviction that confiscation stands as one of the most effective tools against organized crime. By stripping these activities of their profitability, the incentive to continue engaging in criminal conduct diminishes.

Articles 127, 127 *quarter* and 127 *quinquies* of Spanish Criminal Code (hereinafter, “**SCC**”) establish several types of confiscation, depending on their effects:

a. Direct confiscation (Articles 127.1 and 127.2 SCC)

This type of confiscation constitutes a criminal sanction, resulting in the permanent deprivation of proceeds, and is linked to certain penalties: (i) intentional offences, and (ii) negligent offences punishable by imprisonment exceeding one year, although in the latter case, confiscation remains at the Court’s discretion.

b. Substitute confiscation (Article 127.3 SCC)

The SCC establishes a specific type of confiscation in two scenarios: (i) when proceeds derived directly or indirectly from a criminal offence, those used to commit it, or the profits obtained from its perpetration cannot be located; and (ii) when the current value of these assets and profits is lower than at the time of their acquisition.

In such cases, the Spanish legislator allows for the confiscation of other assets belonging to the defendant, even if they bear no connection to the criminal activity under prosecution and are of lawful origin.

c. Third-party confiscation (Article 127 *quater* SCC)

The institution of confiscation extends beyond the proceeds within the defendant's estate. It may also apply to third parties who, despite not participating in the commission of the criminal offence, hold ownership or possession of assets or profits connected to it.

However, at least one of the following conditions must be met: (i) third parties knew or suspected the illicit origin of the proceeds; or (ii) they should have known or suspected such origin. Furthermore, the first condition shall be presumed *iuris tantum* if the assets were acquired by third parties either free of charge or for a price below market value.

Additionally, substitute confiscation may apply to other assets belonging to third parties if they conceal or transfer the original assets.

d. Extended confiscation (Article 127 *quinquies* SCC)

While the previously analysed types of confiscation are imposed through a judgment alongside a criminal conviction, extended confiscation may be ordered beforehand. This allows the Court to deprive the defendant of certain proceeds whose illicit origin has not yet been proven.

Extended confiscation requires the fulfilment of the following conditions:

- (i) A criminal conviction for any offence listed in Article 127 *bis*.1 of the SCC (e.g., human trafficking, organ trafficking, money laundering, tax fraud, private-sector corruption, bribery, etc.).
- (ii) The commission of the criminal offence in the context of prior or ongoing criminal activity.
- (iii) The existence of reasonable suspicion that a significant part of the proceeds derives from criminal activity. Such suspicion may arise from circumstances including:
 - i. Disproportion between lawful income and suspected illicit gains.
 - ii. Use of intermediaries, legal entities, or tax havens to conceal assets.
 - iii. Transfer or disposal of assets aimed at obstructing their traceability.
- (iv) Reasonable suspicion that the illicit profits exceed €6,000.

e. Confiscation without conviction (Article 127 *ter* SCC)

In certain cases, the illicit origin of the assets may be proven during the proceedings. However, due to specific circumstances related to the defendant — such as death, severe illness, absconding, or the extinction of criminal liability — the criminal proceedings cannot continue.

In such situations, the SCC allows the Court to order the confiscation of assets and profits even in the absence of a conviction.

Enforcement of Judgments

Lastly, asset recovery may proceed through enforcing a criminal conviction. This conviction holds the defendant liable for civil compensation and/or the confiscation of proceeds linked to the offence. These include assets used in its commission and any profits obtained from criminal activity.

Whether civil compensation has been duly established and proven during trial phase – primarily through expert reports – and the judgment orders compensation on this basis, two distinct scenarios may arise: (i) the judgement specifies the amount of compensation to be awarded, or (ii) the judgment imposes civil liability without determining the *quantum* of the compensation.

In the first case, the enforcement of the compensation will be governed by the precautions observed in Spanish Civil Procedure Code, which provides the requirement of payment and even the possibility of seizure of assets.

In the second scenario, Article 794 SCPC provides a procedure by which the amount of compensation can be individualized at the enforcement stage of the judgment. To this end, parties may submit any evidence and arguments they deem appropriate. As in the first scenario, the Spanish Civil Procedure Code applies. Consequently, the enforcement of the judgment may involve a requirement of payment and, where appropriate, the seizure of assets.

Even if the criminal conviction is not final yet, Article 989 SCPC provides the possibility to initiate **provisional enforcement** of the civil liability arising from the criminal offence. To this end, Article 989 SCPC refers to the Spanish Civil Code Procedure.

Fraudulent Conveyance

As a final safeguard, to strengthen the enforcement of asset recovery measures, Spanish criminal law provides for a specific criminal offence as a coercive measure to prevent asset stripping. This offence, known as fraudulent conveyance, carries a prison sentence ranging from one to four years, as established in Article 257.2 of the SCC.

Additionally, this offence establishes the criminal liability of the legal entity for which the perpetrator works. Liability arises if the entity benefits from the unlawful conduct and lacks an effective Crime Prevention Model. Such a model must be capable of preventing the commission of the offence.

This offence may be deemed committed in relation to any asset depletion activities carried out by the perpetrator, even if criminal proceedings have not yet been instituted.



ICC FraudNet
Global Annual Report 2025

Part IV: Cybercrime

iccfraudnet.org

ICC | **FraudNet**

ICC FraudNet
Global Annual Report 2025

Emerging Cyber Security Challenges in Poland

JOANNA BOGDAŃSKA

iccfraudnet.org





Emerging Cyber Security Challenges in Poland

Joanna Bogdańska
KW Kruk and Partners

Abstract

This article examines the evolving cyber security landscape in Poland, emphasizing recent surges in hacker activity, the misuse of artificial intelligence ('AI'), and vulnerabilities associated with emerging technologies. Given Poland's growing geopolitical significance, these developments have notable implications for white collar crime lawyers engaged in cross-border investigations, asset recovery, and corporate compliance advisory.

Introduction: Surge in Cyber Attacks

Cyber security threats have escalated dramatically in Poland over the past two years. As a result, lawyers specializing in white collar crime must adapt to a rapidly changing environment where financial crime increasingly intersects with cybercrime. Poland's experience illustrates broader global trends while presenting distinct regulatory and operational challenges.

Poland recorded over 600,000 cyber security incidents in 2024, representing a 62% year-over-year increase.¹ The most frequent attacks include:

¹ See; CERT Polska, *Annual Cyber Security Report 2024*, available at: <https://cert.pl/en/posts/2025/04/annual-report-2024/> (accessed 20 May 2025)

- **Phishing and Smishing Campaigns:** phishing accounted for 94.7% of all reported incidents. Smishing attacks (SMS-based phishing) saw an unprecedented rise, with over 355,000 incidents, reflecting a 60% year-over-year growth.
- **Ransomware Attacks:** Ransomware attacks increasingly targeted financial institutions, healthcare providers, and government agencies. Several Polish banks, including regional cooperative banks, experienced significant operational disruptions due to ransomware demands.
- **DDoS Attacks:** Distributed Denial of Service (‘DDoS’) attacks intensified against public service websites – notably airports, energy providers, and municipal government portals. Such attacks, often politically motivated, sought to disrupt public trust and operational continuity.

State-sponsored groups, particularly those aligned with Russian interests, have been linked to many of these incidents, as cyber conflict continues to parallel geopolitical tensions.²

Analysis of attack vectors revealed that:

- Over 70% of phishing emails were designed to steal online banking credentials.
- Nearly 30% of ransomware infections involved initial access via Remote Desktop Protocol (‘RDP’) vulnerabilities.
- DDoS attacks were primarily sourced from botnets located outside the European Union, complicating attribution and legal recourse.

Poland’s increasing exposure to cyber threats is attributed not only to its geopolitical positioning but also to digital transformation across industries, which often outpaces the implementation of robust cyber security measures.

The Emergence of AI-Driven Cyber Threats

Artificial intelligence technologies have introduced a new class of cyber threats:

- **Automated Phishing:** Cybercriminals leverage AI to craft highly personalized phishing emails and SMS messages at scale. Natural language processing (‘NLP’) models enable the creation of content that mimics authentic communication styles, increasing click-through and compromise rates. It is estimated that AI-enhanced phishing attempts have a 45% higher success rate compared to traditional phishing.
- **Deepfake Technology:** AI-generated deepfakes (manipulated audio, images, and video) are increasingly used in social engineering attacks. Recent incidents in

² See: CyberDefence24.pl, Analysis of Geopolitical Cyber Threats in Poland, 2024.

Poland have involved deepfake videos impersonating CEOs to authorize unauthorized financial transfers.

- **Adaptive Malware:** Machine learning algorithms enable malware to adjust its behavior dynamically in real time, evading traditional detection methods such as signature-based antivirus programs. Adaptive malware can analyze its environment and alter its execution strategy based on observed defenses.
- **AI-Driven Password Cracking and Vulnerability Exploitation:** Tools enhanced with AI can predict passwords or identify system vulnerabilities far more efficiently than human hackers, reducing the time needed to breach secure networks.

As generative AI models become more accessible, the sophistication and frequency of AI-assisted cyber attacks will continue to escalate. In Poland, cybersecurity agencies have observed early trends of AI being used not only by organized crime groups but also by politically motivated hackers.

Vulnerabilities Introduced by Emerging Technologies

The rapid deployment of emerging technologies in Poland, while offering significant operational efficiencies and innovation, has simultaneously created new and complex vulnerabilities that are increasingly exploited by cybercriminals.

Key areas of concern include:

Internet of Things (‘IoT’) Devices

The widespread adoption of IoT devices—such as smart meters, connected cameras, industrial sensors, and personal health monitors—has expanded the attack surface exponentially.

- **Inadequate Security by Design:** Many IoT devices are manufactured with minimal security protections, lacking basic features like encryption, secure boot mechanisms, or regular patch updates.
- **Botnet Formation:** Compromised IoT devices are frequently weaponized into botnets, such as Mirai variants, to conduct massive DDoS attacks against businesses and critical infrastructure.
- **Supply Chain Risks:** Vulnerabilities at the component or firmware level can be introduced during manufacturing, often outside Poland, complicating accountability and remediation efforts.

Cryptocurrency Ecosystems

Poland has witnessed a surge in the adoption of cryptocurrencies for both legitimate and illicit purposes:

- **Anonymity and Obfuscation:** Cryptocurrencies like Monero and privacy-enhancing tools (mixers and tumblers) enable cybercriminals to launder proceeds of fraud, bribery, and embezzlement with reduced traceability.
- **Exchanges and Regulation Gaps:** While larger crypto exchanges now comply with Anti-Money Laundering/Know-Your-Customer ('AML/KYC') standards, smaller or offshore platforms continue to operate with minimal oversight which present challenges for asset tracing and recovery.
- **Smart Contract Vulnerabilities:** In DeFi platforms, coding flaws or governance loopholes have been exploited to siphon millions in assets without traditional legal recourse.

Cloud Computing Risks

Migration to cloud environments, accelerated by the pandemic and remote work trends, presents critical exposure points:

- **Misconfigured Cloud Services:** Human error in configuring cloud storage or access permissions remains a leading cause of data breaches in Poland.
- **Shared Responsibility Confusion:** Many companies misunderstand that while cloud providers secure the infrastructure, the customer remains responsible for securing the data and applications.
- **Insider Threats and Credential Theft:** Stolen or misused credentials for cloud accounts can allow attackers to exfiltrate sensitive corporate data without triggering traditional perimeter defenses.

Emerging technologies thus demand an evolution not only in cyber defenses but also in legal strategies addressing white collar crime and asset protection.

Regulatory and Legal Framework Developments

Poland's regulatory response to the rapidly evolving cyber threat landscape has progressed notably over recent years. However, several systemic challenges remain that white collar crime practitioners must carefully navigate when advising clients or pursuing cross-border investigations.

Delayed Implementation of the NIS2 Directive

The European Union's NIS2 Directive, designed to strengthen cyber resilience across critical sectors, imposed a transposition deadline of 17 October 2024. Poland, however, failed to meet this deadline, with full legislative implementation still pending in early 2025. Key issues arising from the delay include:

- **Regulatory Uncertainty:** Organizations operating in sectors considered "essential" or "important" (e.g., financial services, energy, health, and digital infrastructure) face uncertainty about compliance obligations.
- **Inconsistent Enforcement:** Until full alignment with NIS2 occurs, regulatory oversight is fragmented between different national bodies, complicating incident reporting, supervisory procedures, and enforcement actions.
- **Increased Liability Exposure:** Companies may be simultaneously subject to outdated Polish regulations and newer EU expectations, leading to overlapping or conflicting legal responsibilities.

Fragmented Institutional Oversight

Cyber security in Poland involves multiple regulators and agencies, including:

- The **Ministry of Digital Affairs** (coordinating national cyber security policy),
- The **Office of Electronic Communications ('UKE')** (overseeing telecommunications security),
- **CERT Polska** (the incident response center),
- The **Personal Data Protection Office ('UODO')** (supervising GDPR compliance).

This fragmentation can result in:

- **Duplicative Reporting Requirements:** Organizations may have to report the same incident to multiple authorities.
- **Inconsistent Guidance:** Differing interpretations of cyber security obligations can hinder timely compliance.
- **Jurisdictional Conflicts:** Particularly when incidents involve cross-border data breaches or multinational operations.

New Criminal Law Initiatives

Poland has introduced or proposed several criminal law initiatives to enhance deterrence and enforcement in cyber crime contexts, including enhanced penalties for unauthorized access to IT systems, data theft, and cyber sabotage and introduction of criminal liability for legal entities. Draft legislative proposals foresee expanding corporate criminal liability for serious cyber security failings, including negligent failure to prevent cyber attacks.

Recognizing the challenges posed by digital evidence and the speed of cyber operations, Polish legislators have proposed and partially implemented a series of new procedural tools aimed at enhancing law enforcement's ability to investigate, preserve, and prosecute cyber-related offenses. These tools represent a significant shift in the legal landscape and have direct implications for white collar crime lawyers:

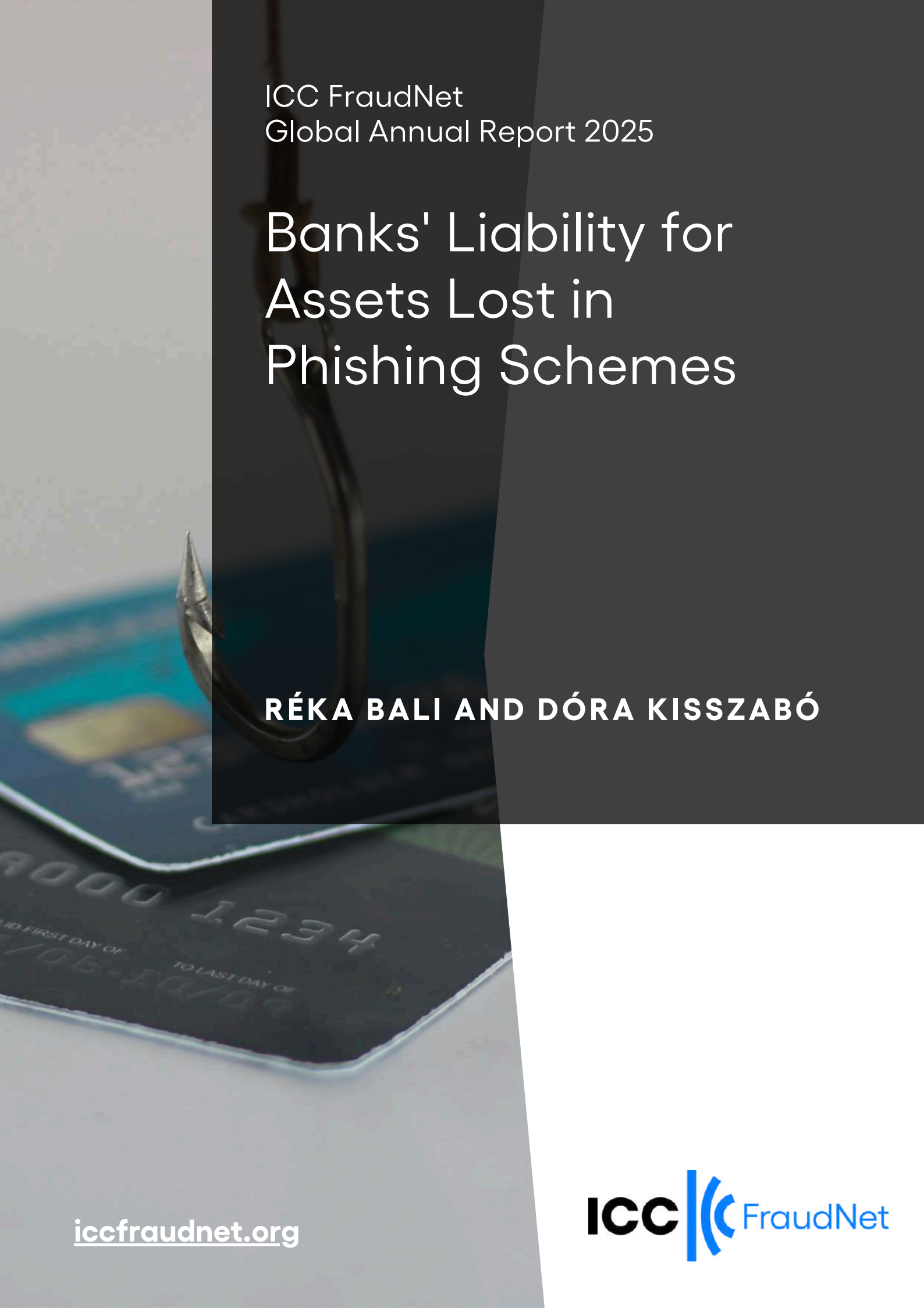
- **Expedited Data Preservation Orders:** Under proposed amendments to the Polish Criminal Procedure Code, prosecutors and courts may issue expedited data preservation orders requiring Internet Service Providers ('ISPs'), cloud service providers, and digital platforms to immediately preserve specific categories of data relevant to an investigation. This includes metadata, server logs, content data (such as emails or messages), and blockchain transaction records. Providers may be required to act within a matter of hours upon receipt of the order. Data must typically be preserved for an initial period of 90 days, extendable by judicial authorization.
- **Remote Search and Seizure Authorization:** Legislative reforms also introduce the possibility of remote search and seizure. Law enforcement agencies, upon obtaining court authorization, may conduct remote searches of digital devices and systems suspected of being used to commit cyber offenses. This includes accessing cloud storage, email servers, or even encrypted communications if decryption is feasible under existing technical capacities. The procedures aim to balance investigative needs with fundamental rights by requiring strict oversight, proportionality, and judicial control. Remote searches raise important legal questions concerning privacy rights, attorney-client privilege, and the scope of lawful surveillance—particularly relevant when digital evidence involves communications between legal counsel and clients.

- **Cross-Border Data Requests and Cooperation:** Following Poland's commitment to international frameworks such as the Budapest Convention on Cybercrime and ongoing EU initiatives, new procedural norms facilitate:
 - Streamlined Mutual Legal Assistance ('MLA') for cross-border cyber investigations, allowing faster requests for digital evidence located abroad.
 - Use of the European Production Order ('EPO'): When fully implemented, Polish authorities will be able to compel providers in other EU Member States to produce specified electronic evidence directly, bypassing slower MLA channels.

Although these changes are positive steps, they also create greater exposure for businesses and their executives, especially regarding the sufficiency of internal cyber security measures.

Conclusion

Poland's cyber security landscape offers a critical and dynamic case study in the evolving convergence of financial crime and technology. For white collar crime lawyers, adapting to this new environment means developing deeper technological expertise, understanding the regulatory nuances, and working closely with cyber forensic professionals. Those who proactively integrate cyber risk considerations into their practices will be better positioned to protect their clients' interests and manage complex cross-border challenges.



ICC FraudNet
Global Annual Report 2025

Banks' Liability for Assets Lost in Phishing Schemes

RÉKA BALI AND DÓRA KISSZABÓ



Banks' Liability for Assets Lost in Phishing Schemes

Réka Bali and Dóra Kisszabó
Forgó Damjanovic & Partners

Introduction

Anyone who banks online has no doubt heard of phishing scams, which target unsuspecting customers by luring them to fake websites that mimic banks' official platforms to steal their authentication details. When such frauds are successful, banks typically point the finger at the customers themselves, claiming that it was their own negligence in disclosing their data that led to the damage. In this article, we would like to present the recent decision of the Hungarian supreme judicial body ('Curia') (case number: Pfv.I.20.685/2024.), which shows a new approach in judicial practice by limiting the banks' ability to avoid liability and emphasising their obligation to compensate the customer for the amount lost due to online fraud.

The Facts of the Relevant Case

The wronged party of the case was a customer, who – in line with today's popular trend – wished to sell an item on an online platform dedicated to the sale of second-hand products. Upon receiving a message in the online platform app, the customer gave their e-mail address to a potential buyer. Shortly after, they received an e-mail containing a link, which navigated to a platform showing a remarkable resemblance to the customer's online banking website.

The customer filled out their login information on this fake site, which resulted in them receiving an SMS from their real bank with a confirmation code. The customer entered this code on the fake website without reading the SMS carefully. They then received

another SMS to authorize a transfer of 1 HUF (approx. 0.0025 EUR), which the fraudster described as a "trial transfer" for the sale.

The customer later discovered that approximately HUF 1.5 million (approximately EUR 3,700) was missing from their account. As they had not authorised such a second transfer, they initiated the bank's complaint procedure and asked for a reimbursement, which the bank refused.

It turned out that when the customer thought they had authorized the login, it actually also meant authorizing a new mobile app registration, and when they thought they had authorized the "trial transfer" of 1 HUF, it also meant registering the fraudster as a secure partner. In this way, the fraudster could later make transfers to their own account without additional authorisation being needed from the accountholder.

The customer filed a complaint with the Financial Arbitration Board ("FAB"), operated by the Hungarian National Bank as an alternative dispute resolution platform, claiming that the bank should reimburse him for the unauthorised transfer. The FAB ruled that the bank should refund the money, as the SMS sent to the customer to authorise the "trial transfer" did not mention that someone should also be registered as a secure partner, which later resulted in the fraudster being able to transfer money from the customer's account.

The bank appealed against the FAB's decision, arguing that it was the customer who had been grossly negligent in providing their details to the fake website, thereby allowing the fraudster to access their bank account, and that it was therefore exempt from liability for the loss. This was in line with previous case law, which typically exempted banks from such liability.

Legal Background

According to the Hungarian legislation on payment service providers, the customer and all persons having access to the customer's bank account have an obligation to ensure the security of the authentication data necessary for accessing the account. This obligation consists of "acting in a manner normally expected in the given situation", which is also the standard of general diligence in Hungarian law.

Payment service providers, such as banks, are generally liable to reimburse customers for damage resulting from transfers that were not duly authorized by the accountholder. Banks are, however, exempt from this liability if the damage was caused by the customer's deliberate or grossly negligent breach of the obligation to keep their authentication data secure.

Like in many other online phishing scam cases, this legal provision served as the basis for the Curia's analysis in the relevant decision. The judges interpreted many notions that are key to adjudicating further online fraud cases, such as whether entering data

on a fake site in and of itself constitutes grossly negligent behaviour in terms of keeping one's data safe. In previous practice, this rule was used by banks to refuse countless reimbursement requests, claiming that if the customer disclosed their data to the fraudster, they were automatically grossly negligent. So far, there was no court practice that limited banks in doing so.

The Curia's Assessment

While the first instance confirmed the bank's liability for the damage, the second instance exempted the bank, deeming the customer's conduct grossly negligent. After these conflicting decisions of lower courts, the Curia as the supreme judicial forum decided to side with the first instance court.

The Curia affirmed that the negligent nature of a certain behaviour is a question of law, not of facts. Furthermore, it stated that the condition for the bank's exemption consists of two elements, namely that (i) the customer does not act diligently (in a manner normally expected in the given situation), and that (ii) this constitutes gross negligence on their part. The Curia also clarified that the grossly negligent behaviour must be in relation to the damage, not the breach of the duty of care itself.

The Curia also confirmed that the criterion of diligence is to be examined on an objective basis, by assessing whether the given customer acted as it is expected of an average, reasonably informed and cautious person. Whereas the criterion of gross negligence is completely subjective and requires the examination of the specific person's awareness of the potential consequences and their emotional attitude towards avoiding the risk.

According to the supreme judicial forum's analysis, the second instance court erred in considering the two criteria as one by deducting that if the customer did not act diligently (i.e. in providing their data on a fake site), it automatically translates to gross negligence. The second instance court also failed to analyse the customer's subjective attitude towards the damage: whether they should have known that damage is going to occur as a result of their behaviour and whether they were so severely negligent that they almost wished for this outcome.

Examining the facts of the case, the Curia concluded that the customer could not have foreseen the occurrence of the damage, and that their conduct cannot be deemed as grossly negligent. For example, they could not have been expected to know that they are going to be a victim of fraud by a potential buyer asking for their e-mail address, because it would have been possible that the buyer only wanted to negotiate the sale via e-mail. Similarly, the customer could not have been expected to realise that they are not on their bank's official platform. Even providing their login details was not negligent on their part, as there are different payment constructions and it could have been possible that a login was required in order to accept payment.

The customer was found to have been somewhat negligent in not reading the bank's SMS thoroughly enough. However, according to the Curia, this did not rise to the level of "gross" negligence, especially since the second SMS from the bank did not contain the registration of a secure partner in addition to the "trial transfer". All in all, therefore, the Curia found that the bank could not be exempted from its obligation to reimburse the amount lost as a result of a phishing scheme, since the customer had not been grossly negligent in foreseeing the damage.

Conclusion

This decision of the Curia is an important milestone in the practice of online fraud cases. It was generally well received by society, with many newspapers describing it as the Curia "siding with the customers against the banks". This assessment is not far from the truth: by emphasising that entering one's authentication details on a fake bank website does not automatically exempt the bank from reimbursing the amount lost, the Curia's decision could change the course of many similar cases in the future. Especially as lower courts are obliged to follow the Curia's interpretation.

According to the Hungarian National Bank, there are more than ten thousand successful online fraud attempts in Hungary every year.¹ Following the decision in this matter, banks may not continue their previous practice of invoking the customer's gross negligence simply because he or she did not realise that he or she was on a fake site. From now on, banks will also have to prove that the customer was aware of the potential damage and knowingly disregarded the risk - a task that may prove difficult, given that most frauds are successful only because customers genuinely fail to recognise the fraudulent elements.

¹ See: <https://www.mnb.hu/sajtoszoba/sajtokozlemenyek/2025-evi-sajtokozlemenyek/kiberccsalasi-ugyben-nyert-pert-a-kurian-a-penzugyi-bekelteto-testulet> (accessed 20 June 2025)

ICC FraudNet
Global Annual Report 2025

Ransomware Attacks in Japan 2024

**HIROYUKI KANAE AND
HIDETAKA MIYAKE**

iccfraudnet.org





Ransomware Attacks in Japan - 2024

**Hiroyuki Kanae & Hidetaka Miyake
Anderson Mori & Tomotsune**

Ransomware Attacks in Japan in 2024

According to Trend Micro, the number of reported cases of ransomware attacks against Japanese companies and organizations has been increasing year by year, reaching a record 84 cases in 2024.¹ Meanwhile, according to the National Police Agency, the number of reported cases of ransomware attacks in the first half of 2024 was even higher, at 114 cases.²

As for the characteristics of ransomware attack targets in 2023, there were many cases in which organizations with weak IT infrastructure such as small and medium-sized companies and hospitals were targeted. However, since 2024, ransomware attacks have also been seen in companies with strong IT infrastructure systems, such as those operating in the distribution industry, in the IT industry, and in the education industry.

One relatively large-scale attack was a ransomware attack on Izumi Co., Ltd. in May, 2024. In this incident, it was announced that the personal information of 7.78 million cardholders may have been leaked.³

1. See: https://www.trendmicro.com/ja_jp/jp-security/25/a/securitytrend-20250108-01.html (accessed 2 March 2025)

2. See: https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf (accessed 2 March 2025)

3. See: <https://www.izumi.co.jp/corp/ir/pdf/2024/0509news.pdf> (accessed 9 March 2025)

In July 2024, Tokio Marine & Nichido Anshin Life Insurance announced that information of policyholders and former employees may have been leaked due to a ransomware infection that originated at its tax accounting firm, Takano Sogo Accounting Office.⁴ The information that was leaked included the personal information relating to 27,824 contracts, including the names of policyholders and their insurance premiums, and the personal information of 82 former employees, including the names of retirees, their retirement payment amounts, and monetary claims.

In addition to ransomware attacks, cyber-attacks recorded between the end of 2024 and the beginning of 2025 also targeted critical infrastructures such as transportation, airlines, and social infrastructure companies such as banks. The trend of attacks targeting social infrastructure systems is an ongoing problem.

Details of Ransomware Attack on KADOKAWA

In early June 2024, KADOKAWA CORPORATION was hit by a ransomware attack, causing massive damage. The cause of the attack was a phishing attack by means of which access to an employee account was stolen, after which the company network was breached.⁵

The breach of information caused by the ransomware infection was extensive, and the personal information of about 254,241 people was leaked. The leaked information included information on all Dwango employees, some of its business partners, current students and alumni of educational organizations using the Internet, such as N Junior High School and N High School, as well as information pertaining to the students and parents of KADOKAWA Dwango Academy. Some contracts and internal documents of Dwango and affiliated companies were also leaked.

Related services were also seriously affected. Several services, including NicoNico, were suspended, and the official website became unavailable.

KADOKAWA's official website and its book-related websites were restored in August 2024, and NicoNico was reopened in October 2024. In this way, the attack resulted in the suspension of services at N High School for 2 months, with a major impact on the online education system.

Notably, the ransomware attack against KADOKAWA was launched by Blacksuit, an upstart group.⁶ Blacksuit has been around since May 2023 and is believed to belong to a Russian hacking group. Its targets range from banking to manufacturing, but recently

4. See: https://www2.tmn-anshin.co.jp/download/1048/240710_news.pdf (accessed 9 March 2025)

5. See: <https://group.kadokawa.co.jp/information/media-download/1347/f4a4b93c03cb933c/> (accessed 9 March 2025)

6. See: https://www.trendmicro.com/ja_jp/jp-security/24/g/expertview-20240716-01.html (accessed 2 March 2025)

healthcare, education and IT sectors have become more vigilant in relation to the threat this group poses.

Blacksuit claimed responsibility for the attack in June with the following email:

“Our team gained access to the KADOKAWA network almost a month ago. It took some time, because of the language, to figure out that KADOKAWA subsidiaries’ networks were connected to each other and to get through all the mess KADOKAWA’s IT department made there. We have discovered that KADOKAWA networks architecture was not organized properly. (...) We don’t think that KADOKAWA’s top management would like to spend a following few months being in excuses. Such exercises do not fit them at all. It would be much easier to pay and keep moving forward for such a company as KADOKAWA is. ALL DATA will be released on July 1st.”

It should be noted in the above quote that Blacksuit made it clear in the details of their intrusion that the ransom offered by KADOKAWA was too low, and that it would release business information, including personal information, if it did not accept further ransom negotiations. It is not clear whether KADOKAWA paid the ransom, but the main feature of this case is how the criminal group revealed the inside story behind the ransom negotiations.

Lessons from the KADOKAWA Ransom Attack

There are organizational factors, human factors, and technical factors that caused the cyber incidents at KADOKAWA.

(1) Organizational and technical factors

One of the factors is that KADOKAWA's network architecture was not properly organized. In other words, different networks were connected to one large KADOKAWA infrastructure and controlled through global control points such as eSXI and V-sphere. Therefore, once an attacker accessed the control center, the entire network could be decrypted.

In addition, it is possible that vulnerabilities in external contacts such as public servers and VPN devices were exploited in this attack and allowed the intrusion. Some of the vulnerabilities in VPNs were able to steal authentication information used for access, leading to the authentication breach. As a preventive measure, the fundamental solution seems to be to update the firmware to eliminate vulnerabilities that can be attacked.

(2) Human Cause

The cause of the attack was that an employee's account information was stolen by a phishing attack whereupon the company's network was breached. From this point of

view, it is necessary to conduct inhouse IT security education on a regular basis to raise employees' awareness of phishing attacks. In addition, there was insufficient IT personnel within the enterprise with sufficient hacking-related know-how.

As described above, this cyber-attack was carried out by finding vulnerabilities in the system due to a combination of organizational and technical factors, as well as due to human factors. In order to build a defence system, it is necessary to identify the above factors and eliminate all of them.

Closing Remarks

It has been announced that the loss due to the above ransomware attack on KADOKAWA is expected to cost approximately 3.6 billion yen for recovery costs and creator compensation costs. It has also been announced that the impact on the business results for the fiscal year ending March 2025 is expected to be a decrease of 8.4 billion yen in sales and 6.4 billion yen in operating income.⁷

In this case, the stock price of KADOKAWA dropped from 3,365 yen on June 7, the day before the incident, to 2,580 yen on June 28 (20 days after June 9, 2024 when the company announced that the outage was caused by a cyber-attack including ransomware and that it would take more than 1 month to recover), a drop of more than 20%. In this way, we can see how a company that is hit by a ransomware attack will potentially not only have to pay a large amount of money to recover its operations, but must also expect to bear the costs of compensating its users and, on top of all of this, bear the triple burden of experiencing a significant decline in the value of its shares.

Although it is impossible to completely defend against a ransomware attack, the losses for an enterprise once it is hit by a ransomware attack can be staggering. Therefore, in spite of the significant investments required by an enterprise in its security operations and infrastructure, such costs are clearly worth every penny.

7. See: <https://group.kadokawa.co.jp/information/media-download/1332/8dd990c3e531706d/> (accessed 10 March 2025)



ICC FraudNet
Global Annual Report 2025

Recovering Funds from Chinese Onshore Banks for Foreign Telecom- Fraud Victims

ANDY LIAO

iccfraudnet.org





Recovering Funds from Chinese Onshore Banks for Foreign Telecom-Fraud Victims

Ronghua (Andy) Liao
Han Kun Law Offices

Overview

An increasingly common cross-border telecom fraud scheme has emerged in China in recent years. The scheme is typically perpetrated by fraudsters who establish a foreign shell company outside mainland China through which they open a non-resident bank account (“NRA account”) with a mainland Chinese bank (the “receiving bank”). Using various pretexts, the fraudsters induce foreign enterprises or individuals to instruct their overseas remitting bank to transfer funds into the NRA account. Once these funds arrive, the fraudsters transfer them into an ordinary foreign-currency account at the receiving bank or another domestic bank, convert the foreign currency into local currency through foreign exchange settlement, and dissipate the funds through layered transactions.

In such cases, the core challenge lies in the speed and complexity of the fund movements and the specificities of Chinese laws and practices, which are causing significant obstacles for overseas victims in recovering their losses in such cases. This article proposes targeted recovery methods at each stage of the fund flow and illustrates how to coordinate administrative supervision with practical legal tools. It systematically explores the strategies and measures by which victims of international telecom fraud can recover their funds through Chinese legal proceedings.

Cross-Border Fund Flows and Underlying Legal Relationships

Cross-border telecom fraud typically involves a multi-jurisdictional flow of funds that begins with the victim's account at the remitting bank and then to the receiving bank with intermediaries in between, such as correspondent banks. Upon receipt by the receiving bank, the funds flow to the fraudster's NRA account in mainland China at the receiving bank, which are transferred to a general foreign exchange account with the receiving bank or another financial institution. After this, the fraudsters convert the funds into local currency and proceed to dissipate the funds.

The involvement of intermediary banks depends on whether the remitting and receiving banks maintain correspondent settlement agreements or mutual accounts. Typical scenarios include the following.

1. *The receiving bank holds an account at the remitting bank.* Upon the victim's remittance instruction, the remitting bank debits the victim's account and credits the receiving bank's account held at the remitting bank. The remitting bank then issues a payment advice to the receiving bank, which releases the funds to the fraudster's NRA account.
2. *The remitting bank maintains an account at the receiving bank.* The remitting bank debits the victim's account and authorizes the receiving bank to debit its own account. The receiving bank subsequently transfers the funds to the fraudster's NRA account.
3. *No direct nostro/vostro account relationship exists between the remitting bank and the receiving bank.* In this case, direct clearing is not possible, and thus an intermediary bank is introduced. This intermediary bank usually maintains accounts with both the remitting bank (or its correspondent bank) and the receiving bank (or its correspondent bank), thereby acting as a bridge between the remitting and receiving banks.

To execute these transfers, banks rely on international messaging and settlement systems—most notably SWIFT (Society for Worldwide Interbank Financial Telecommunication) and clearing systems such as CHIPS (Clearing House Interbank Payments System). As a global financial communications network, SWIFT is primarily responsible for transmitting standardized payment instructions between banks but does not handle the actual transfer of funds. Payment systems such as CHIPS enable net settlement across multiple banks to process fund transfers. In cross-border remittances, common SWIFT message types include MT103 (Customer Transfer), MT202 (General Financial Institution Transfer), etc. An MT103 message typically includes information about the remitter, beneficiary (recipient), instructing bank (originating bank), receiving bank, and intermediary bank (if applicable).

In essence, a remittance is a business operation whereby the remitting bank, acting on the remitter's instructions, delivers funds to the designated recipient through various channels. Although the entities involved may differ depending on the method, the legal relationships in remittance transactions are relatively clear: all parties in the remittance chain form entrustment relationships. Specifically, the remitter and the remitting bank establish entrustment relationships for the remittance, as do the remitting bank and the receiving bank. The recipient and the receiving bank form an agency relationship for fund collection. If intermediary banks are involved, agency relationships also exist between the remitting bank and the intermediary bank, and between the intermediary bank and the receiving bank for fund processing.

Potential Methods of Recovery at Each Stage of the Fraud

Before the defrauded funds have been credited to the receiving account

Numerous factors can affect the speed at which a cross-border remittance is credited to the receiving account. These include whether an intermediary is involved, the nature of the receiving account opened in mainland China, and even whether the remitter is subject to foreign-exchange controls. As a result, by the time the victims realize they have been defrauded, it is possible that the receiving bank has not yet completed the crediting process.

Under prevailing Chinese doctrine, a depositor and a bank have a debtor-creditor relationship, i.e., the depositor holds only a right of claim against the bank for repayment of principal and interest. Thereafter any movement of those funds in the remittance process remains a modification of that underlying claim. A cross-border remittance is an "indicative delivery": the remitter creates a new right of claim in favor of the beneficiary against the receiving bank. Accordingly, so long as the fraudulent funds have not yet been credited, the beneficiary does not yet hold a right to claim against the receiving bank.

As noted above, there exists an entrustment relationship between the remitting bank and the receiving bank with respect to any funds that have been remitted but not yet settled or credited. This means that the remitter and the remitting bank have not yet performed their respective duties and that the beneficiary has not yet acquired a right of claim against the receiving bank. In such cases, victims may consider the following measures to recover their funds.

Promptly issue a request to the receiving bank and report to local law enforcement

When funds have been remitted but not yet credited to the fraudster's account, the receiving bank will typically suspend further processing upon receiving a recall request from the remitting bank. During this process, presenting a police report helps to

demonstrate that the transaction arose from telecom fraud rather than a commercial dispute, thereby resulting in swift cooperation from Chinese banks and the relevant authorities.

As noted earlier, the non-crediting of funds indicates that the remitting bank's entrusted obligations remain incomplete. The victim's prompt issuance of a recall instruction to the remitting bank essentially constitutes a revocation of the remitting bank's obligation to remit the funds. Under Chinese law, the remitting bank may notify the receiving bank to assert its right to unilateral termination of the entrustment relationship with the receiving bank under the *PRC Civil Code*, demanding that the receiving bank return the funds as restitution.

Some Chinese commercial banks have operational guidelines for handling recall requests. For example, the *Agricultural Bank of China Foreign Exchange Remittance Business Operating Procedures* stipulate, "[w]hen the receiving bank receives a recall/revocation request from the remitting bank, it shall handle the matter as follows: (1) If the inbound remittance has not been settled: Halt the settlement, deduct relevant fees per the remitting bank's instructions, and return the funds to the remitting bank..."

Thus, under applicable law, the receiving bank may face no legal impediment to refunding the funds to the original remitter in accordance with the remitting bank's instructions, provided that the funds have not yet been credited into the beneficiary's account. In practice, however, some Chinese domestic receiving banks adopt a cautious stance and, before processing a refund, may require a disclaimer from the remitting bank or supporting documents from competent financial regulatory authorities, public security authorities, or court orders.

Sue the receiving bank to demand a return of funds

Given that the remitting and receiving banks already maintain an entrustment relationship via SWIFT messages, the remitting bank may file suit against the receiving bank in mainland China to insist on a same-route refund. For instance, in the case (2014) Qing Jin Shang Zhong No. 80, the Qingdao Intermediate People's Court of Shandong Province held in its reasoning that: "Before the disputed remittance is settled into the beneficiary's account, the funds do not belong to the beneficiary. The receiving bank's decision to return the funds upon the remitting bank's instructions - based on their agency relationship - is legally permissible."

The situation becomes more complex if the remitting bank refuses to cooperate and the victim must bring a lawsuit in its own name because no direct entrustment relationship expressly exists between them. In this context, China's concept of "undisclosed agency" may apply. Specifically, the victim could argue that the receiving bank, through the SWIFT messages, was aware of the victim's identity when processing the remittance instruction and that the receiving bank should have recognized that the remitting bank acted on the victim's behalf. Thus, an undisclosed agency relationship is established between the victim and receiving bank, making the

agency relationship between the remitting and receiving banks directly binding on the victim and the receiving bank. Through this undisclosed agency framework, the victim may file a lawsuit against the receiving bank to demand fund recovery, even without privity of contract.

Request the receiving bank to return the funds based on instructions from the authorities

As cross-border telecom fraud constitutes a criminal offense, the most common means of recovery lies within China's criminal procedure framework. In criminal cases, Chinese courts generally adhere to the principle of "criminal proceedings precede civil", dismissing civil claims (e.g., unjust enrichment) brought by the victim until the related criminal procedures conclude. Rather, restitution typically occurs during criminal proceedings. For instance, after the illegal or criminal acts have been judicially adjudged, the public security authorities handling the case may directly return the property to the victims or aggrieved parties, provided that: (1) clear and undisputed ownership of the property is supported by conclusive evidence; (2) such restitution does not harm the lawful interests of other victims, aggrieved parties, or third-party stakeholders; and (3) the return of property does not interfere with the normal progress of ongoing investigations or judicial proceedings.

While Chinese law grants domestic authorities jurisdiction over when recipient accounts are located in China, victims of cross-border telecom fraud matters are typically advised to seek relief through mutual legal assistance channels. This is so due to certain factors, including the victim's foreign domicile, the extraterritorial location of the fraud, and investigative difficulties inherent in international cases.

Nevertheless, based on our practical experience, if a preliminary investigation by Chinese authorities confirms the existence of fraud—and recognizing both the clear entitlement of the victim and the procedural complexities faced by foreign complainants—they may issue an informal statement of case facts or similar document recommending that the receiving bank refund the defrauded funds. In such circumstances, once the receiving bank acknowledges the underlying fraud, its legal risk is minimal in honoring the authorities' directives and remitting the funds back via the original payment route, and banks are generally willing to comply.

When Defrauded Funds have been Credited to an NRA Account but Not Yet Dissipated

In cross-border fund transfers, once the receiving bank has credited the beneficiary's account, the beneficiary immediately acquires a deposit claim against the receiving bank. At this stage, absent the beneficiary's consent or a formal court order, the receiving bank normally is reluctant to unilaterally reverse the transfer. Victims in these instances can consider the following means of recovery.

Apply to local authorities for an emergency payment suspension

The mechanism of “emergency payment suspension” derives from the *Notice on Establishing an Emergency Payment Suspension and Rapid Freezing Mechanism for Accounts Involved in New Types of Telecom Network Fraud* (hereinafter referred to as the “*Notice on Emergency Payment Suspension*”). Under this framework, a bank must suspend the payment functions of any account suspected of being used for telecom fraud upon receipt of an instruction from a public security authority and after it verifies the relevant information.

A victim may request an emergency payment suspension either by calling a police hotline or by reporting directly to the bank. There is no requirement that the public security authority file a formal case beforehand. The public security authority will transmit an electronically signed emergency payment suspension order to the head office of the bank where the account to be suspended is held. The bank, through its internal transaction-processing system, will immediately verify the account name, account number, remittance amount, and transaction timestamps against the information contained in the order. If these details are consistent, the bank must suspend all debit and credit operations on the targeted account without delay and may then conduct its own inquiry into the account holder. Each suspension remains in place for 48 hours from the moment of activation, and may be applied up to two times in total. In practice, the process can be completed swiftly from the moment the victim reports the fraud to the undertaking of suspension measures.

During the 48-hour suspension window, the public security authority examines the veracity of the victim’s report. If the report is confirmed as genuine and approved by the responsible public security official, a criminal case is formally filed. Thereafter, via the internal supervisory platform, the public security authority issues a “Notice of Assistance to Freeze Assets” to the head office of the bank holding the suspended account. Upon receipt of this notice, the bank is required to freeze the account. Even after emergency suspension has been implemented, the receiving bank may launch its own due diligence investigation into the beneficiary. Until the beneficiary cooperates to clarify the legitimacy of the transactions, all operations on the account remain suspended. Knowing that the account has been frozen and is under investigation, fraudsters often abandon further transactions from that account. Although an emergency stop does not in itself compel a refund, it serves to preserve any remaining funds and prevents their further dissipation.

Seek a refund from the receiving bank

As noted above, at this stage victims can still seek a statement of case facts or similar document from the authorities; however, once the funds have been credited, it becomes highly uncertain as to both the willingness of the authorities to issue such an informal instruction and the receiving bank’s readiness to act on it. Because the

credited funds constitute the account holder's property interests, neither the public security bureau nor the receiving bank may unilaterally debit the account and effect a refund without the depositor's consent or a binding judicial or regulatory order.

International criminal judicial assistance

Recovery is substantially more difficult at this stage than before the funds have been credited. However, unlike the phase in which the funds have already been dissipated, here the advantage lies in that the money remains in the primary fraud-related account. At this stage, the victim may still petition for international criminal judicial assistance to request cooperation from Chinese authorities in repatriating the funds.

Based on China's legal framework and practical experience, three pathways exist for Chinese authorities to initiate recovery in cross-border telecom fraud cases.

- *INTERPOL channels.* INTERPOL National Central Bureau of China (under the International Cooperation Bureau of the Ministry of Public Security) → Provincial Public Security Authorities → Local/Municipal Public Security Authorities.
- *Diplomatic channels.* Ministry of Foreign Affairs → Ministry of Public Security → Provincial Public Security Authorities → Local/Municipal Public Security Authorities.
- *Mutual Legal Assistance Treaties.* Judicial Ministry's International Cooperation Bureau → Ministry of Public Security → Provincial Public Security Authorities → Local/Municipal Public Security Authorities.

Because all three pathways involve multiple agencies and levels of approval, they are often time-consuming in practice and there is significant uncertainty as to whether the local authorities will ultimately accept the case and provide assistance.

File an unjust-enrichment claim against the recipient

Victims may consider initiating a civil action and preservation of funds in China concurrent with or in lieu of other measures. This is so because of the uncertainties inherent in the means of recovery at this stage - an emergency payment suspension may be lifted, international criminal judicial assistance can be protracted, and that the victim cannot be certain of continued restrictions on the beneficiary account.

While, as noted above, in telecom-fraud cases, Chinese courts typically give precedent to criminal over civil cases and may decline to accept a civil case on this basis. Accordingly, when drafting the case statement and articulating the causes of action, the victim must take great care to present the facts and legal grounds in a manner that avoids the court classifying the suit as a *de facto* criminal proceeding and rejecting it at

filing. It is worth noting, however, that Chinese courts generally do not conduct a substantive review of the merits during the initial case-acceptance and preservation-order stages, focusing instead on formal admissibility.

Defrauded Funds have been Dissipated

In cross-border telecom fraud, fund transfers typically occur quickly. A more probable scenario in practice is that victims realize they have been defrauded only after the funds have already been dissipated. At this stage, the following measures may be considered:

Apply for extended payment suspension

Pursuant to the *Notice on Emergency Payment Suspension*, if the funds have already been transferred out of the initially suspended account, the bank must relay the transfer details to the public security authority. The authority will then decide whether to extend the suspension to any downstream recipient accounts (i.e., secondary or lower-tier), a process known as an “extended suspension”. If the authority elects to proceed, it will issue an Extended Emergency Payment Suspension Notice to the relevant banks or payment service providers, instructing them to freeze the incoming funds. Each extended suspension remains in force for 48 hours. Where defrauded funds traverse multiple layers of accounts, extensions may be applied at each layer without statutory limitation on the number of tiers.

In 2021, China’s Ministry of Public Security Criminal Investigation Bureau promulgated the *Revised Provisions for Public Security Authorities’ Payment Suspension, Inquiry, and Freeze in Telecom Network Fraud Cases*. Under these provisions, the authority to review and execute payment suspension orders was delegated to the public security organ at the same administrative level as the unit receiving the initial report, significantly accelerating the review and execution process. The Revised Provisions also introduced an automatic tracing and extended suspension mechanism: when a bank provides complete transfer information, an extended suspension is triggered automatically. This enhancement streamlines previous workflow in the Notice on Emergency Payment Suspension, “fund transfer → feedback to public security bureau → bureau decision → extended suspension”, and turns it into a faster, more automated procedure.

Claim tort liability compensation from the receiving bank

Whether the receiving bank bears tort liability depends on whether it was negligent in handling the remittance or its ancillary services, the principal form of such fault being a breach of the laws and regulations governing financial conduct. Crucially, the basis for such liability arises from separate factual grounds unrelated to the telecom fraud itself (e.g., procedural violations in account opening or fund settlement) - each constitutes a separate legal fact - and the former does not depend on the outcome of

the latter. Thus, a Chinese court should not refuse to hear a tort action against the receiving bank based on the “criminal proceedings precede civil” principle.

To determine whether the receiving bank violated applicable regulatory requirements, the inquiry focuses principally on two aspects of its operations: the account-opening process and the fund settlement (payment-execution) process.

- *Account opening phase.* The bank must verify the account holder’s identity through multiple channels, rigorously review the authenticity, completeness, and compliance of corporate account documentation, and implement know your client (KYC) principles to ensure clients’ eligibility, identity authenticity, and information accuracy.
- *Fund settlement phase.* The bank must fulfill its KYC and due diligence obligations. This includes identifying the transaction’s background, nature, purpose, compliance and consistency with declared foreign exchange activities; verifying alignment between transaction documents and cross-border fund flows; fulfilling obligations to report large or suspicious transactions; and filing suspicious transaction reports for anomalies exceeding thresholds.

In conclusion, successfully holding the receiving bank liable hinges on case-specific factual and legal analyses, requiring detailed scrutiny. In cross-border transactions, Chinese domestic banks are regulated by multiple authorities, including the People’s Bank of China (PBOC), the State Administration of Foreign Exchange (SAFE), and the National Financial Regulatory Administration (NFRA). Relevant regulatory provisions are also extensive and fragmented, including but not limited to:

- Anti-Telecom and Online Fraud Law of the People’s Republic of China
- Anti-Money Laundering Law of the People’s Republic of China
- Regulations of the People’s Republic of China on Foreign Exchange Administration
- Circular of the People’s Bank of China on Matters relating to Strengthening the Management of Payment and Settlement to Prevent New-type Telecommunication Network Crimes
- Circular of the People’s Bank of China on Matters Concerning Further Enhancing Administration of Payments and Settlement to Guard Against New-type Telecommunication and Online Illegal and Criminal Activities
- Circular of the People’s Bank of China on Strengthening Account-opening Management and the Follow-up Control Measures after Suspicious Transaction Reporting
- Circular of the People’s Bank of China and the State Administration of Foreign Exchange on Issuing the Guidelines for Anti-money Laundering and Counter-terrorism Financing of the Cross-border Business of Banks (for Trial Implementation)

- Circular of the People's Bank of China on Strengthening Client Identification for Anti-money Laundering
- Administrative Measures for the Reporting of Large-value and Suspicious Transactions by Financial Institutions

Under Chinese law, the statute of limitations for bringing a tort claim against a bank is three years, calculated from the date on which the injured party knows - or ought reasonably to have known - both the wrongful act and the identity of the tortfeasor. Victims of telecom fraud are often unaware of any bank misconduct until they undertake further investigation - whether by filing a criminal report or obtaining a lawyer's investigative order - so initiating a civil claim as soon as evidence of the bank's regulatory or tortious breach comes to light will almost always fall within the permissible time frame.

Recovery with Assistance from Regulatory Authorities

During the process of recovering cross-border telecom fraud proceeds, close collaboration with regulatory authorities can compel these agencies to discharge their supervisory responsibilities and expedite oversight of banks and other financial institutions, thereby encouraging banks to cooperate in repatriating victims' funds. In 2015, the State Council established an inter-ministerial joint conference mechanism to combat and address new telecom network crimes. This mechanism comprises twenty-three departments and entities, including the Supreme People's Court, the Supreme People's Procuratorate, the Ministry of Industry and Information Technology, the PBOC, the former China Banking Regulatory Commission (now the NFRA), China Telecom, China Unicom, and China Mobile. In the context of cross-border telecom fraud, this mechanism plays a strategic role in coordinating efforts and pooling resources. The principal financial regulators involved are the PBOC, the SAFE, and the NFRA.

Because fraudsters in these schemes often exploit loopholes in the banking system, victims should proactively seek support from financial regulators. At an early stage, victims frequently face an impasse: banks decline to disclose detailed fund flow information on the grounds of "client confidentiality" and public security authorities defer formal case filing due to jurisdictional complexities. At this juncture, victims should approach the PBOC or the SAFE - either orally or in writing - and present a clear summary of the facts and request that the regulator initiate an investigation into the suspected fraud.

If repeated verbal and written inquiries fail to elicit a substantive response, the victim may submit a formal complaint or dispatch a legal demand letter, highlighting alleged violations of the remitting bank in the NRA account opening or fund disbursement processes. Upon receiving such a complaint or letter, the regulator will likely request preliminary evidence that the bank breached its customer due-diligence or anti-money laundering (AML) obligations. The victim need only supply sufficient information to

substantiate the bank's potential noncompliance and identify the specific regulatory lapses.

For instance, the receiving bank may have violated relevant anti-money laundering laws if the ultimate controller of an NRA account is solely a Chinese national and the bank failed to fulfill its KYC obligations when opening the NRA account, conducting only a perfunctory review of the identity of the shell company's ultimate controller; or if in cross-border trade transactions, the bank neglected to scrutinize forged trade documents, thereby failing to verify the authenticity, consistency, and legality of the transactions; or if the bank did not file a Suspicious Transaction Report for abnormally large foreign exchange settlement transactions.

If the regulatory authorities are persuaded to launch an internal inquiry, the findings can not only trace the subsequent flow of the defrauded funds but also uncover the bank's unlawful or noncompliant behavior during stages such as account opening and transaction monitoring. These findings can serve as crucial evidence in subsequent civil litigation to hold the bank liable for torts. Moreover, if the funds have not yet been settled, the regulatory scrutiny and intervention exerts considerable pressure on the bank: to avoid administrative sanctions - such as fines or suspension of its foreign-exchange business license - for failing to fulfill its foreign exchange authenticity verification duties, the bank may be incentivized to negotiate a voluntary repayment with the victim.

Legal Instruments for Cross-Border Fund Recovery

In recovering defrauded funds, as noted above, the most common scenario is that by the time a victim discovers the fraud, the funds have already been dissipated. The victim may nonetheless initiate a civil action against the responsible bank without being constrained by the "criminal proceedings precede civil" principle. Within such civil proceedings, the following legal tools can be synergized with other remedial measures to improve the prospects of recovery.

Property Preservation

China's property preservation mechanism functions similarly to the freezing order or Mareva injunction in common-law jurisdictions. It comprises three stages - pre-litigation preservation, litigation preservation, and pre-enforcement preservation - creating a layered mechanism to prevent debtors from dissipating assets during litigation or enforcement.

Pre-litigation preservation allows a party to freeze the opposing party's assets prior to filing suit or arbitration, provided it posts security equal to 100% of the requested preservation amount (e.g., in cash or via a bank/insurance guarantee). The court must rule on this application within 48 hours. Litigation preservation is applicable when a

case is accepted and remains pending until judgment, a party may request preservation by posting security, which is typically 30% of the preservation amount. In practice, pre-litigation and litigation preservation processes have largely merged. Plaintiffs commonly submit preservation applications together with their case-filing materials. The case-filing and trial divisions of courts then coordinate internally to accept the case and render a decision within five days, after which the enforcement division executes the preservation order *ex parte*, without prior notice to the respondent (e.g., seizure, freezing, or attachment of assets). Consequently, a notable procedural hurdle for international victims is the requirement to notarize and authenticate their identity and authorization documents when initiating litigation in China, which may delay the opportunity to secure timely preservation orders.

The evidentiary threshold for asset preservation is lower than that of a freezing order under common law. The applicant need not prove a *prima facie* case in full but must show that exigent circumstances exist, and that failure to preserve assets immediately would cause irreparable harm to their legitimate interests. Acceptable forms of security include cash deposits or litigation liability insurance policies, with premiums typically ranging from 0.04% to 0.08% of the preservation amount. Insurers will generally assess the facts of the case, legal risk, and evidentiary sufficiency before underwriting such policies.

In cross-border telecom fraud cases, victims may apply for preservation orders to freeze assets under the control of the fraudster, including secondary or downstream accounts not yet subject to extension payment suspension by police. This requires that the victim first identify the downstream accounts controlled by the fraudster - an effort that typically involves tools such as a lawyer's investigation order.

Investigation Orders

Investigation orders in China serve a role similar to that of several common law disclosure tools, including disclosure orders, Norwich Pharmacal orders, and Bankers Trust orders. These orders are designed to assist victims in tracing the flow of defrauded funds to recovery. However, unlike their common law counterparts, which impose disclosure obligations on respondents or third-party banks by court order, the Chinese system is more victim-initiated: the court grants the victim's lawyer authority to conduct an investigation, but the onus is on the lawyer to collect the necessary evidence by directly engaging with the relevant institutions. This tool is not yet enshrined in national legislation but is authorized by judicial regulations issued at the provincial or municipal level.

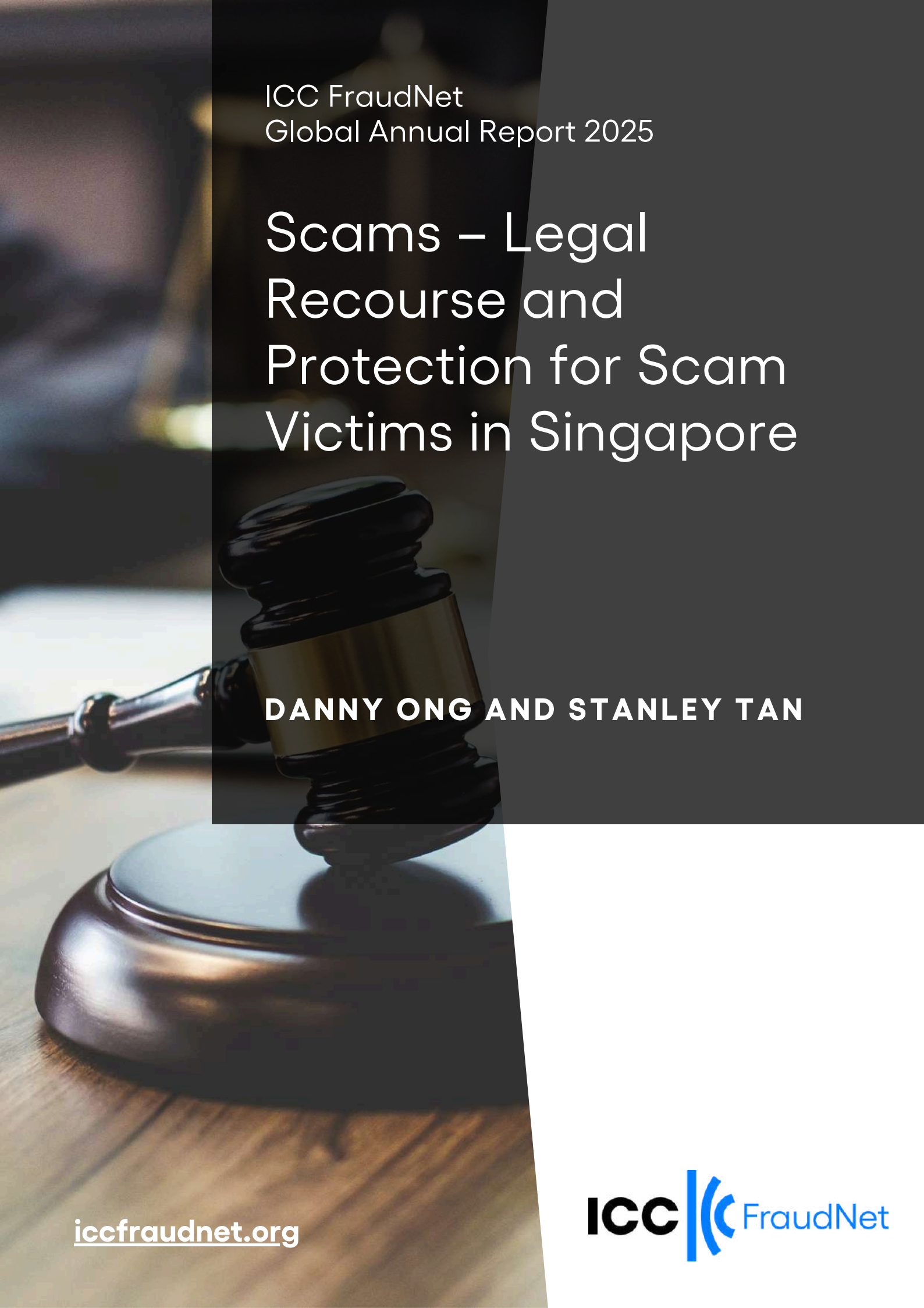
In cross-border telecom fraud cases, investigation orders are primarily used to trace the destination of the defrauded funds. Unlike a Bankers Trust order, which requires the bank to proactively search for related accounts, the victim must provide the court with the specific bank account numbers and the names of the banks to be investigated. Victims typically know at least the details of the primary account. By analyzing the

transaction history of that primary account, the victim can progressively identify secondary, tertiary, and lower-tier accounts, and then apply for successive investigation orders to uncover the flow of funds. Based on these findings, the victim can apply for property preservation measures or pursue compensation directly against the holders of the implicated accounts.

Conclusion

Cross-border recovery of telecom fraud funds is an inherently complex, system-wide endeavor that demands multidimensional coordination of legal procedures, collaboration with financial regulatory authorities, and strategic application of legal instruments. From the perspective of the fund flow, every link in the chain offers potential avenues for legal recourse - from the remitting bank to intermediary banks, to the receiving bank, and ultimately to downstream domestic accounts. Successful recovery hinges on deploying precise strategies at each stage of the fund flow, coupled with proactive regulatory involvement. Victims must operate within the legal framework, leverage a tailored combination of tools, and utilize communication channels with public security authorities and financial regulators to surmount obstacles and reclaim their losses.

Finally, it is worth noting that defrauded funds from telecom-fraud schemes from many years past may still lie dormant in onshore accounts or internal ledgers due to China's foreign exchange controls, banks' internal compliance with anti-fraud and anti-money laundering measures, and the operational restrictions domestic banks may place on beneficiary accounts. Even if victims previously abandoned their recovery efforts due to procedural or practical obstacles, they may retain the right to the means of recovery described above to reclaim those funds.



ICC FraudNet
Global Annual Report 2025

Scams – Legal Recourse and Protection for Scam Victims in Singapore

DANNY ONG AND STANLEY TAN

iccfraudnet.org

ICC |  **FraudNet**



Scams – Legal Recourse and Protection for Scam Victims in Singapore

Danny Ong and Stanley Tan
Setia Law

Abstract

The surge in scams globally has not spared Singapore, which in 2024 witnessed an alarming S\$1.1 billion in scam-related losses, a staggering 70% spike from the previous year.¹ As scams grow in scale and sophistication, so too must the legal and regulatory strategies that confront them. In this article, Danny Ong and Stanley Tan of Setia Law LLC examine the potential avenues available under Singapore law for victims seeking recovery, and also comment on recent legislative and regulatory initiatives aimed at preventing scams and providing recourse to scam victims.

Introduction

Scams represent a persistent and deeply corrosive threat to society – they not only inflict financial devastation and emotional harm on victims and their families, but also impose systemic costs on the state as national resources have to be diverted to absorb and remediate the financial fallout. To effectively combat scams, jurisdictions must

¹ Natasha Ganesan, “At least S\$1.1 billion lost to scams in 2024; one victim had S\$125 million stolen” *Channel News Asia* (25 February 2025) <<https://www.channelnewsasia.com/singapore/scams-cybercrime-1-billion-one-victim-125-million-crypto-4956461>>, accessed on 23 June 2025.

adopt comprehensive strategies that extend beyond prevention, and also seek to implement legal frameworks that empower victims to recover losses from scammers and hold accountable the key intermediaries that serve as critical gatekeepers in the fight against scams. This article examines the legal framework in Singapore available to victims to pursue recovery, and also comments on some of the legislative and regulatory measures implemented by the Singapore government to counter the growing menace of scams.

Pursuing Claims Against Scammers

In the aftermath of a scam, victims typically focus their initial recovery efforts on pursuing the scammers themselves, and Singapore law offers a robust suite of civil remedies and reliefs for such victims. Depending on the specific circumstances of the scam, victims may bring claims against the scammers and their accomplices for, among other things, unjust enrichment,² the tort of deceit,³ the tort of conversion,⁴ dishonest assistance,⁵ knowing receipt,⁶ and/or unlawful means conspiracy.⁷

In appropriate cases, victims may also seek urgent interim relief from the Singapore courts to prevent the further dissipation of stolen assets and/or to facilitate asset tracing. These include freezing and proprietary injunctions,⁸ as well as disclosure orders against third parties such as financial institutions or custodians believed to have received or processed the proceeds of fraud,⁹ even where such parties are located outside Singapore.¹⁰ The Singapore courts have also demonstrated a readiness to grant such relief in respect of digital assets, including cryptocurrency,¹¹ which scammers frequently exploit due to its anonymity and ease of transfer.

However, while Singapore law offers victims a suite of reliefs and remedies that can be used against scammers, they may not always yield results. This is particularly true in today's landscape, where scammers are increasingly skilled at concealing their identities and laundering stolen assets. Victims also often only become aware that they have been scammed after a significant delay, by which time tracing and recovering the misappropriated funds may be exceedingly difficult, even with the above-mentioned legal tools.

² *Benzline Auto Pte Ltd v Supercars Lorinser Pte Ltd* [2018] 1 SLR 239 at [45].

³ *Panatron Pte Ltd and another v Lee Cheow Lee and another* [2001] 2 SLR(R) 435 at [14];

⁴ *Tat Seng Machine Movers Pte Ltd v Orix Leasing Singapore Ltd* [2009] 4 SLR(R) 1101 at [45]-[47]; *Ong Teck Soon (executor of the estate of Ong Kim Nang, deceased) v Ong Teck Seng & another* [2017] SGHC 95 at [18]-[22].

⁵ *George Raymond Zage III and another v Ho Chi Kwong and another* [2010] 2 SLR 589 (“*George Raymond*”) at [20].

⁶ *George Raymond* at [23].

⁷ *CLM v CLN and others* [2022] SGHC 46 (“*CLM*”) at [72].

⁸ *CLM* at [48] & [56].

⁹ *CLM* at [57]-[60].

¹⁰ Singapore Supreme Court Practice Directions 2021 at [63(3)(u)].

¹¹ *CLM*; *Janesh s/o Rajkumar v Unknown Person (“CHEFPIERRE”)* [2022] SGHC 264.

Pursuing Claims Against Financial Institutions

When recovery against scammers proves futile, victims may naturally wish to consider pursuing claims against their banks or financial institutions (“FIs”) to recoup their losses. Victims may try to sustain such claims on grounds that their FIs were negligent and/or breached an implied contractual term to take reasonable care by failing to block the transfer of funds to scammers. However, as will be discussed below, pursuing and succeeding in these claims present significant challenges.

First, victims risk having such claims summarily dismissed on the ground that their FIs owe no duty to block transfers that their customers have authorised. Although there is no Singapore judgment directly on point, UK jurisprudence supports the position that no such duty exists. In *Philipp v Barclays Bank UK plc* [2023] UKSC 25 (“*Philipp*”), a victim of an authorised push payment (“APP”) scam sued her bank for failing to refuse her payment instructions, which led to £700,000 being paid to scammers. The UK Supreme Court summarily dismissed the claim, holding that a bank’s duty of care does not extend to questioning its customer’s authorised instructions,¹² unless there is reason to believe the customer lacked mental capacity or that an agent was acting fraudulently.

Second, even if victims manage to resist summary dismissal of their claims by persuading the Singapore court to take a different approach from *Philipp*,¹³ they will still face an uphill battle in establishing that their FIs should compensate them for their losses. This is because the burden is placed entirely on victims to establish the standard of care expected of their FIs on the specific facts of their case, convince the Singapore Court that their FIs had failed to meet this requisite standard, and prove that this failure had caused their losses. Unless victims can point to clear evidence that their FIs have fallen short of industry standards¹⁴ and that their loss would have been avoided if those standards were met, succeeding against their FIs in court will prove challenging.

Furthermore, it may also be impractical for victims to pursue their claims against FIs in court. Having already suffered significant financial losses, victims may be reluctant or unable to incur further costs in pursuing litigation against their FIs, especially in circumstances where the likelihood of success is uncertain for the reasons outlined

¹² *Philipp v Barclays Bank UK plc* [2023] UKSC 25 (“*Philipp*”) at [100].

¹³ See *Hsu Ann Mei Amy v Oversea-Chinese Banking Corp Ltd* [2011] 2 SLR 178 where the Singapore High Court suggested at [23] that a bank had a broad duty to “take reasonable care in all the circumstances”. See also, *Zheng v Bank of China (Canada) Vancouver Richmond Branch* [2023] BCJ No. 144 at [42] where the British Columbia Court of Appeal declined to summarily dismiss the claimant’s case, as it recognised that it was possible for the defendant bank to owe a duty to inquire and warn its customer of a potential scam before processing a large payment request.

¹⁴ *BNM (administratrix of the estate of B, deceased) on her own behalf and on behalf of others v National University of Singapore and another* [2014] 2 SLR 258 at [63]; *Tradewaves Ltd and others v Standard Chartered Bank and another suit* [2017] SGHC 93 at [166]; *Zeus Aircraft Owner 2 Limited and another v Polar Pay Limited* [2023] HKCU 5068 at [29].

above. This practical limitation likely accounts for the absence of reported cases involving such claims in Singapore.

Pursuing Claims Through the Shared Responsibility Framework

An alternative to court proceedings that potentially offers scam victims a more cost-effective and expeditious route to recover their losses is the Shared Responsibility Framework (“SRF”).

The SRF is an initiative by the Monetary Authority of Singapore (“MAS”) and the Infocomm Media Development Authority of Singapore (“IMDA”) that requires FIs and telecommunication service providers (“Telcos”) to implement prescribed anti-scam safeguards. Where a victim’s losses arise from a FI’s failure to comply with its prescribed obligations under the SRF, the FI is expected to provide compensation. Conversely, if the FI has discharged its duties but the Telco has not, the responsibility for compensation shifts to the Telco. If both the FI and the Telco are compliant, the SRF cannot be used to seek redress and the victim will have to rely on other avenues (e.g. the courts) for recovery.

Under the SRF, FIs are required to:¹⁵

- impose a 12-hour cooling-off period where high-risk activities¹⁶ cannot be performed after a digital security token is activated on a device, or a new device is used to log into a payment account;
- provide real-time notifications when digital tokens are activated, a new device is used to log into a payment account, and/or when high-risk activities are carried out;
- provide real-time notifications when outgoing transactions are made;
- provide a 24/7 reporting channel and a self-service feature which allows the account holder to block further access to his/her account;
- provide real-time fraud surveillance directed at detecting unauthorised transactions in a phishing scam; and

¹⁵ Monetary Authority of Singapore & Infocomm Media Development Authority, *Guidelines on Shared Responsibility Framework* (24 October 2024) (“Guidelines on SRF”) at section 4.2.

¹⁶ “high-risk activities” is defined in section 2.1 of the Guidelines on SRF to mean the “(a) adding of payees to the account holder’s payment profile; (b) increasing the transaction limits for outgoing payment transactions from the payment account; (c) disabling transaction notifications that the responsible FI will send upon completion of a payment transaction; and (d) changes in the account holder’s contact information including mobile number, email address and mailing address”.

- if a protected account¹⁷ is being drained of a material sum,¹⁸ to block the transaction and all subsequent transactions until it is able to obtain further verification from the account holder, or send a notification to the account holder and hold the transaction for at least 24 hours.

Telcos are required under the SRF to:¹⁹

- only deliver text messages with Sender IDs (i.e. the display name of the sender) to subscribers if the text messages originate from authorised aggregators. Authorised aggregators are organisations licensed by the IMDA who will conduct checks to ensure that all text messages with Sender IDs that they process come from senders who are registered with the Singapore SMS Sender ID Registry (“**SSIR**”) and authorised to use the relevant Sender ID. The effect of this is that Singapore users will now no longer receive text messages from scammers who try to defraud Singapore users by using the same Sender IDs as legitimate organisations; and
- implement an anti-scam filter to block text messages containing malicious URLs from being delivered to its subscribers.

Victims who pursue recovery through the SRF need not be concerned about funding their claims, because the SRF places the onus on the relevant FIs and Telcos to investigate the victims’ claims and duly compensate the victims under the SRF if appropriate. Victims need only initiate a claim with their FIs, who are obliged to inform the relevant Telco (where applicable). Both the FI and Telco are thereafter required to appoint officers, who are independent of their business units, to assess the victim’s claim and determine whether any breach of their duties under the SRF has occurred. Investigations must be concluded within 21 business days for straightforward cases and within 45 business days for more complex matters.²⁰ Victims will also be provided with a written outcome of the investigations and can pursue other avenues of recovery against their FIs and/or Telcos if they are dissatisfied with the outcome.

It should, however, be noted that the SRF cannot be used to pursue recovery against FIs and Telcos for all types of scams. The SRF only covers scams perpetrated through the impersonation of a legitimate business or government entity, where the scammer obtains the victim’s credentials using a fabricated digital platform and performs

¹⁷ A “protected account” is defined in section 2.1 of the Guidelines on SRF to mean “any payment account that (a) is held in the name of one or more persons, all of whom are individuals; (b) is capable of having a balance of more than S\$1,000 (or equivalent amount expressed in any other currency) at any one time, or is a credit facility; (c) is capable of being used for electronic payment transactions; and (d) where issued by a relevant payment service provider, is a payment account that stores specified e-money.”

¹⁸ According to Guidelines on SRF at p. 7, a protected account is considered to be rapidly drained of a material sum if “(a) the protected account has account balance of S\$50,000 or more immediately prior to the seemingly authorised transaction and (b) more than 50% of such account balance is transferred out within the last 24 hours.”

¹⁹ Guidelines on SRF at section 5.2.

²⁰ Complex cases may include cases where any party to the seemingly authorised transaction is overseas and uncontactable during the investigation period, see Guidelines on SRF at section 7.9.

transactions that the victim did not intend.²¹ It does not, for example, cover scams where victims themselves are deceived into authorisation payments themselves as was in the case of *Phillip*, malware scams, or phishing through non-digital means (e.g. phone calls or face-to-face meetings).

If the type of scam in question falls outside the scope of the SRF, victims will have to pursue their claims against FIs and/or Telcos through other avenues. Though in such cases, the prescribed duties outlined within the SRF – which are, in some respects, applicable in the prevention of a broader range of scams – may still serve as a valuable reference point when arguing whether FIs or Telcos have breached their duties owed to their customers and should therefore compensate them for their loss.

Protection from Scams Act 2025

In addition to the SRF, which focuses on the allocation of responsibilities between FIs, Telcos, and victims in the aftermath of a scam, Singapore has also made concerted efforts in the prevention of scams. For example, the Protection from Scams Act 2025 (“PFSA”) that was passed in Parliament on 7 January 2025 will, after it comes into force, empower police officers to issue restriction orders to banks to prevent scam victims from transferring, withdrawing, and/or drawing down on any credit facility.

The PFSA was initiated because despite extensive public education efforts, a high number of scam cases still involve individuals who willingly authorise the transfer of monies to scammers despite the advice of family, friends, their banks, and even the police – whom until the PFSA comes into force – has no legal powers to stop banks from complying with their customers’ instructions to transfer funds to scammers if they insist on doing so.²² For example, in April 2024, despite efforts by OCBC Bank and the police to talk a scam victim out of transferring S\$130,000 to scammers, the victim refused to comply and insisted on making the transfer.²³ Having exhausted all avenues of persuading the victim otherwise, OCBC eventually allowed the transaction to go through after the victim signed an indemnity form confirming that she knew the risks involved. The victim only realised she had been scammed 2 months later, by which time the transferred funds were lost and she was only left with S\$600 in her accounts.

Therefore, while some critics may characterise the PFSA as overly draconian, its necessity is underscored by the need to protect individuals from falling victim to their own misjudgement as illustrated above. It must also be remembered that the harm

²¹ See definition of “*seemingly authorised transaction*” in the Guidelines on SRF at section 2.1.

²² *Singapore Parliamentary Debates, Official Report* (7 January 2025) vol 95 (Ms Sun Xueling, the Minister of State for Home Affairs), <<https://sprs.parl.gov.sg/search/#/sprs3topic?reportid=bill-735>>, accessed on 23 June 2025.

²³ Nadine Chua, “We couldn’t save her from herself: How scam victim went from \$130k in savings to \$600 in 2 months” *The Straits Times* (24 November 2024) <<https://www.straitstimes.com/singapore/we-couldnt-save-her-from-herself-how-scam-victim-went-from-130k-in-savings-to-600-in-2-months>>, accessed on 23 June 2025.

inflicted by scams transcends the immediate financial losses suffered by individual victims, often reverberating through their families and, by extension, placing strain on public resources. In some instances, victims have found themselves unable to meet their financial needs and have turned to the Government for assistance, a concern that was expressly acknowledged during the Second Reading of the PFSA in parliament. The PFSA is therefore a critical instrument in Singapore's broader efforts to combat scams, and it is hoped that it will stem the significant outflow of funds lost to scams once it comes into force.

Conclusion

In conclusion, the surge in scams across the world underscores the pressing need for jurisdictions to not only implement robust preventive measures, but also put in place legal frameworks that empower victims to seek redress and involve key intermediaries in the fight against scams. Singapore is no exception as can be seen from the recent implementation of the SRF and the enactment of the PFSA. While these measures represent meaningful progress, continued efforts and innovation will be essential, as scammers persist in developing methods to circumvent existing safeguards and as novel scam typologies continue to emerge.

ICC FraudNet
Global Annual Report 2025

Part V: Tackling Fraud, Corruption and Money Laundering

iccfraudnet.org





ICC FraudNet
Global Annual Report 2025

Recovery of Looted State Properties – An Analysis of Ghana's Latest Asset Recovery Attempt

**BOBBY BANSON AND ISAAC
AKYERIFI-MENSAH JNR**



Recovery of Looted State Properties – An Analysis of Ghana’s Latest Asset Recovery Attempt

Bobby Banson and Isaac Akyerifi-Mensah Jnr.

Introduction

Ghana's political landscape has consistently battled with corruption, with the recovery of looted state assets being one of the critical issues. Post-independence, successive governments have struggled with recovery of looted state assets. Each administration has approached this and corruption as a whole with its own strategies as is evident in the approaches of the major political parties, the New Patriotic Party (NPP) and the National Democratic Congress (NDC).

In 2016, then-presidential candidate Nana Addo Dankwa Akufo-Addo of the NPP pledged to establish the Office of the Special Prosecutor through an Act of Parliament. This initiative aimed at investigating and prosecuting specific corruption cases, including alleged breaches of public procurement regulations among others.¹ More recently, during his campaign for the just ended elections, H.E. John Dramani Mahama, leader of the NDC, outlined a new anti-corruption strategy in his party's manifesto. He proposed "Operation-Recover-All-Loot" ('ORAL'), with the aim to

¹ Enoch Darfah Frimpong, 'Akufo-Addo to appoint Special Prosecutor to deal with corruption' (www.graphic.com.gh 12 December, 2016) < <https://www.graphic.com.gh/news/general-news/akufo-addo-to-appoint-special-prosecutor-to-deal-with-corruption.html> > accessed 10 April, 2025.

investigate, prosecute, and recover the proceeds of corruption among others.² These initiatives are introduced alongside existing legal frameworks that address various forms of corruption and corruption-related offenses.

This Article will discuss the latest attempt to fight corruption and recover looted state assets; ORAL. This will be done by examining the existing legal framework on the recovery of state properties, institutions charged with investigating, prosecuting and the recovery process. Further discussion will be on the scope of ORAL, its legality and usefulness in line with the existing Whistleblowers Act, 2006 (Act 720) and other existing legal frameworks for combating crimes against the State.

Legal Framework on Recovery of State Properties

There are several legislations that criminalize corrupt acts and omissions that result in the looting of state property. These legal provisions establish the foundation for efforts for the recovery of looted state assets. Further, the Whistleblower Act, 2006 (Act 720), empowers individuals to make disclosures on suspected corrupt activities (which the Act refers to as improprieties), thereby facilitating and providing necessary information for the recovery of state assets. These legislations will be discussed below.

- **The Criminal Offences Act, 1960 (Act 29)**

To begin, the preamble of the Criminal offences (Amendment) Act, 1993 provides that it is “*An act to amend the Criminal Offences Act, 1960 (Act 29) ... to include special offences relating to loss of state funds ...*”³ As a result, Section 3 of the Act inserted Section 179A in Act 29⁴, to criminalize causing loss or damage to state property. Section 179A of Act 29 states as follows:

“179A. Causing loss, damage or injury to property

(1) A person who by a wilful act or omission causes loss, damage or injury to the property of a public body or an agency of the Republic commits a criminal offence.

(2) A person who in the course of a transaction or business with a public body or an agency of the Republic intentionally causes damage or loss whether economic or otherwise to that body or agency commits a criminal offence.

(3) A person commits a criminal offence through whose wilful, malicious or fraudulent action or omission

(a) the Republic incurs a financial loss, or

² The National Democratic Congress (NDC), ‘RESETTING GHANA, NDC 2024 <<https://manifesto.johnmahama.org/files/shares/Resetting%20Ghana%20NDC%20Manifesto%202024.pdf>> p 136, accessed 10 April, 2025.

³ Criminal Offences (Amendment) Act, 1993 (Act 458)

⁴ Criminal Offences Act, 1960 (Act 29)

(b) the security of the Republic is endangered.

(4) In this section “public body” includes the Republic, the Government, a public board or corporation, a public institution and a company or any other body in which the Republic or a public corporation or other statutory body has a proprietary interest.”

The import of the above is that, a person commits a crime if that person, by his action or inaction, whether in the course of a transaction or business, with or without malicious or fraudulent intent, conducts him or herself in a way that causes loss or damage to the property, economic or financials of the state or a public body.

- **The Public Procurement Act, 2003 (Act 663)**

The Public Procurement Act, 2003, (Act 663) as amended by the Public Procurement (Amendment) Act, 2016, (Act 914) also criminalizes certain actions which are not in accordance with standard procurement procedures.

The Act provides in Section 92 as follows;

“Offences relating to procurement

92. (1) A person who contravenes a provision of this Act commits an offence and where a penalty is not provided for the offence, that person is liable on summary conviction to a fine not exceeding two thousand five hundred"" penalty units or a term of imprisonment not exceeding five years or to both the fine and the imprisonment.

(2) The following also constitute offences under this Act:

(a) entering or attempting to enter into a collusive agreement, whether enforceable or not, with any other supplier or contractor where the prices quoted in their respective tenders, proposals or quotations are or would be higher than would have been the case had there not been collusion between the persons concerned;

b) directly or indirectly influencing in any manner or attempting to influence in any manner the procurement process to obtain an unfair advantage in the award of a procurement contract;

(c) altering a procurement document with intent to influence the outcome of a tender proceeding and this includes but is not limited to

a) forged arithmetical correction; and

b) insertion of documents such as bid security or tax clearance certificate which were not submitted at bid opening; and

(d) request for clarification in a manner not permitted under this Act.”

- **The Whistleblowers Act, 2006 (Act 720)**

The preamble of the Act provides that it is “*AN ACT to provide for the manner in which individuals may in the public interest disclose information that relates to unlawful or other illegal conduct or corrupt practices of others; to provide for the protection against victimisation of persons who make these disclosures; to provide for a Fund to reward individuals who make the disclosures and to provide for related matters.*”

Section 1 of the Act provides to the effect that a person may make a disclosure of information where that person has reasonable cause to believe that the information tends to show:⁵

- (a) an economic crime has been committed, is about to be committed or is likely to be committed;⁶
- (b) another person has not complied with a law or is in the process of breaking a law or is likely to break a law which imposes an obligation on that person;⁷
- (c) a miscarriage of justice has occurred, is occurring or is likely to occur;⁸
- (d) in a public institution there has been, there is or there is likely to be waste, misappropriation or mismanagement of public resources;⁹
- (e) the environment has been degraded, is being degraded or is likely to be degraded; or¹⁰
- (f) the health or safety of an individual or a community is endangered, has been endangered or is likely to be endangered.¹¹

Investigative and Prosecutorial Institutions for the Recovery of State Assets

There are several anti-corruption institutions set up by the Constitution and Acts of parliament with the power and mandate of investigating and prosecuting corruption and corruption-related offences which includes the recovery of looted state assets. Some of these institutions will be discussed below.

- **Commission on Human Rights and Administrative Justice (‘CHRAJ’)**

Established under the 1992 Constitution, CHRAJ serves as an independent body mandated to investigate human rights abuses, administrative injustices, and corruption. Article 218 provides one of the functions of CHRAJ as “*to investigate all instances of alleged*

⁵ Section 1, Whistleblower Act, 2006 (Act 720)

⁶ Ibid Section 1(1)(a)

⁷ Ibid Section 1(1)(b)

⁸ Ibid Section 1(1)(c)

⁹ Ibid Section 1(1)(d)

¹⁰ Ibid Section 1(1)(e)

¹¹ Ibid Section 1(1)(f)

*or suspected corruption and the misappropriation of public moneys by officials and to take appropriate steps, including reports to the Attorney-General and the Auditor-General, resulting from such investigations.”*¹² Consequently, this is repeated in the Commission on Human Rights and Administrative Justice Act, 1993 (Act 456).¹³ In addition, the Act provides for other functions such as to investigate allegations that a public officer has contravened or has not complied with a provision of Chapter Twenty-four (Code of Conduct for Public Officers) of the Constitution.¹⁴

- **Office of the Special Prosecutor**

The Office of the Special Prosecutor (‘OSP’) was established under the Office of the Special Prosecutor Act, 2017 (Act 959) as an independent anti-corruption agency with the mandate to investigate and prosecute cases of corruption and corruption-related offenses. The establishment of the OSP was a response to the perceived inefficiency of existing anti-corruption agencies, particularly the Attorney General’s Department, which was often constrained by political influences. The object of the Office includes:

- a) Investigating and prosecuting specific cases of alleged or suspected corruption and corruption-related offences¹⁵
- b) Recovering proceeds of corruption and corruption-related offence¹⁶
- c) Taking steps to prevent corruption.¹⁷

To achieve the above objects, the Act provides for several functions of the Office of the Special Prosecutor. This is provided for in Section 3 of the Act and states as follows:

‘Functions of the Office

3. (1) To achieve the object, the Office shall

(a) investigate and prosecute cases of alleged or suspected corruption and corruption-related offences under the Public Procurement Act, 2003 (Act 663);

(b) investigate and prosecute allegations of corruption and corruption-related offences under the Criminal Offences Act, 1960 (Act 29) involving public officers, politically exposed persons and persons in the private sector involved in the commission of the offence;

¹² Article 218(e), Constitution of Ghana, 1992

¹³ Section 8(f), the Commission on Human Rights and Administrative Justice Act, 1993 (Act 456)

¹⁴ Ibid Section 8(e)

¹⁵ Ibid Section 2(a)

¹⁶ Ibid Section 2(b)

¹⁷ Ibid Section 2(c)

(c) investigate and prosecute alleged or suspected corruption and corruption-related offences involving public officers, politically exposed persons and persons in the private sector involved in the commission of the offence under any other relevant law;

(d) recover and manage the proceeds of corruption;

(e) disseminate information gathered in the course of investigation to competent authorities and other persons the Office considers appropriate in connection with the offences specified in paragraphs (a) and (b), (co-operate and coordinate with competent authorities and other relevant local and international agencies in furtherance of this Act;*

(g) receive and investigate complaints from a person on a matter that involves or may involve corruption and corruption-related offences;

(h) receive and act on referrals of investigations of alleged corruption and corruption-related offences by Parliament, the Auditor-General's Office, the Commission on Human Rights and Administrative Justice, the Economic and Organised Crime Office and any other public body; and

(i) perform any other functions connected with the object of the Office.”

- **Economic and Organised Crime Office**

The Economic and Organised Crime Office (‘EOCO’) is established by the Economic and Organised Crime Office Act, 2010 (Act 840)¹⁸ with various functions including but not limited to investigating and on the authority of the Attorney-General prosecuting serious offences that involve financial or economic loss to the Republic or any State entity institution in which the State has financial interest¹⁹ and recover the proceeds of crime²⁰ among others.

- **The Office of the Attorney-General**

The Constitution provides for there to be an Attorney-General of Ghana who shall be a Minister of State and the principal legal adviser to the Government.²¹ The Constitution further provides for several other functions of the Attorney-General which includes being responsible for the initiation and conduct of all prosecutions of criminal offences.²² In the exercise of this function, the Attorney-General has the power to delegate some of his/her prosecutorial power to other individuals and entities. This is how institutions like the OSP and the EOCO obtain their mandate to investigate and prosecute various offences.

¹⁸ Section 1, Economic and Organised Crime Office, 2010 (Act 840)

¹⁹ Ibid Section 3(a)(i)

²⁰ Ibid Section 3(b)

²¹ Article 88(1), Constitution of Ghana, 1992

²² Article 88(3), Constitution of Ghana, 1992

Oral - Scope and Mandate

On 18th December, 2024, as a preparatory step to recovering proceeds of corruption, the then President-Elect, John Dramani Mahama, set a team to receive and gather information from the general public on suspected acts of corruption.²³ Samuel Okudzeto Ablakwa, the Chairperson of the ORAL Team, has provided clarity to the scope and mandate of ORAL. He states that, the scope of ORAL is strictly limited to gathering and analysing evidence of corruption, rather than acting as judge or prosecutor.²⁴ This limits the scope of the team to an evidence-collection mechanism aimed at empowering relevant state institution.²⁵ In fulfilment of this mandate, the team has set up various platforms and channels through which members of the public can forward information of suspected corrupt acts.²⁶

Did The Then President-Elect Have Such Power To Establish The Oral Committee?

Concerns have been raised as to whether the then President-Elect had any powers to establish the ORAL committee prior to officially assuming office. The primary legislation relevant for this discussion is the Presidential (Transition) Act, 2012 (Act 845). The preamble of the Act states that it is “*AN ACT to establish arrangements for the political transfer of administration from one democratically elected President, to another democratically elected President, to provide for the regulation of the political transfer of power and for related matters.*”

The Act provides for the incumbent president together with the President-Elect to appoint a transition Team for the purposes of the Act. Section 1(1) of the Act states that:

“1(1) Within twenty-four hours after the declaration of the results of the presidential election in accordance with article 63 of the Constitution,

(a) the incumbent President shall appoint

(i) the head of the presidential staff appointed under the Presidential Office Act, 1993 (Act 463),

(ii) the Attorney-General, and

²³ Ernest K. Arhinful, ‘Mahama forms 5-member team to collect public reports on suspected corruption cases’ (www.myjoyonline.com 18 December, 2024) <<https://www.myjoyonline.com/mahama-forms-5-member-team-to-collect-public-reports-on-suspected-corruption-cases/>> accessed 10 April 2025.

²⁴ Abubakar Ibrahim, ‘I won’t be a judge in my own court; ORAL is about protecting public purse’ (www.myjoyonline.com 19 December, 2024) <<https://www.myjoyonline.com/i-wont-be-a-judge-in-my-own-court-oral-is-about-protecting-public-purse-ablakwa/>> accessed 10 April 2025.

²⁵ Ibid

²⁶ Kabah Atawoge, ‘ORAL sets up platforms to collect information on suspected corruption’, ([www.citinewsroom.com](https://citinewsroom.com) 20 December, 2024) <<https://citinewsroom.com/2024/12/operation-recover-all-loot-sets-up-platforms-to-collect-information-on-suspected-corruption/>> accessed 10 April 2025

(iii) the Ministers responsible for Presidential Affairs, Finance, the Interior, Defence, Foreign Affairs, Local Government and National Security, and

(b) the person elected as President shall appoint an equal number of persons as appointed under paragraph (a) to constitute a Transition Team that Shall include the Head of the Civil Service, the Head of the Local Government service, the Secretary to the Cabinet and the National Security Co-ordinator.”

The Act also provides for the functions of the Team in Section 2 of the Act. It states that:

“2. The functions of the Team are

(a) to make comprehensive practical arrangements to regulate, in accordance with this Act, the transfer of political power following a presidential election and a general election;

(b) to ensure the provision of daily national security briefings for the person elected as President during the period before the assumption of office by the person elected as President;

(c) to ensure that the salaries, allowances, facilities, privileges and the retiring benefits or awards as determined

(i) by the President under clause (1) of article 71, and

(ii) by Parliament under clause (2) of article 71

and which are due to the holders of the offices specified in article 71 of the Constitution are paid or accorded to those persons without undue delay; and

(d) to undertake any other function which will enable the Team to achieve the object of this Act.”

From the foregoing, the author contends that any powers that a President-Elect may have, are limited by the Presidential (Transition) Act to the shared responsibility with the Incumbent President to appoint a transition team in accordance with the Act, tasked with performing the aforementioned functions. Consequently, a President-Elect lacks the authority to establish any other committee to act on their behalf until they have been sworn in and assumed office. Therefore, the President-Elect at the time could not have legitimately established the ORAL committee to undertake its purported mandate.

Oral Submits its Report

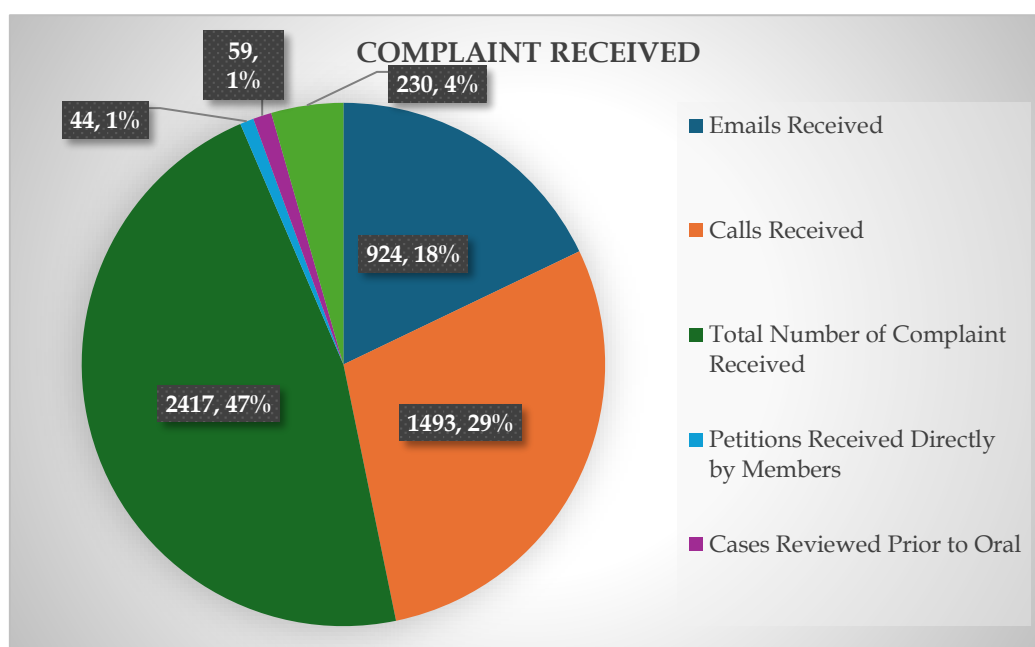
On Monday, 10th February, 2025, the ORAL Team through its Chairman, Samuel Okudzeto Ablakwa, submitted its report to the President containing 2,417 complaints of suspected corruption.²⁷ The committee received 1,493 reports through a toll-free

²⁷ Albert Kuzor, ‘ORAL committee presents report containing 2,417 suspected corruption complaints to Mahama’ (www.myjoyonline.com 10 February, 2025) < <https://www.myjoyonline.com/oral->

call and 924 via emails, bringing the total number of complaints to 2,417.²⁸ According to Sam Okudzeto Ablakwa, the report contains two hundred and thirty cases (230), which have been carefully reviewed and analysed.²⁹ He explains that 59 of these are cases which had come up even before the establishment of ORAL but the team however went back to review those cases.³⁰

According to Mr. Ablakwa, if successful in the recoveries of about 36 high financial cases, a total of 20.49 billion USD can be retrieved and recovered for the state.³¹ He further stated that in respect of looted state lands, if recoveries are successful by inviting the persons involved to pay the fair market price, an estimated amount of 702,000 million USD can be recovered for the state.³²

The President has since referred the report to the Attorney General and Minister of Justice and instructed him to begin probing the cases for further action where necessary.³³



[committee-presents-report-containing-2417-suspected-corruption-complaints-to-mahama/](#) > accessed 10 April 2025

²⁸ Ibid

²⁹ GhanaWeb TV, 'ORAL Committee submits report to Mahama detailing 2,417 suspected corruption complaints' (10 February 2025) < https://www.youtube.com/watch?v=mNmwdy_J8Q&t=221s > accessed 10 April 2025

³⁰ GhanaWeb TV, 'ORAL Committee submits report to Mahama detailing 2,417 suspected corruption complaints' (10 February 2025) < https://www.youtube.com/watch?v=mNmwdy_J8Q&t=221s > accessed 10 April 2025

³¹ Ibid

³² ibid

³³ Albert Kuzor, 'ORAL committee presents report containing 2,417 suspected corruption complaints to Mahama' (www.myjoyonline.com 10 February, 2025) < <https://www.myjoyonline.com/oral-committee-presents-report-containing-2417-suspected-corruption-complaints-to-mahama/> > accessed 10 April 2025

Legitimacy, Usefulness Or Otherwise Of Oral

As stated above, the mandate of ORAL merely involves collecting, gathering and analysing evidence of corruption for the appropriate agency to then deal with it. This is essentially inviting individuals of the public to disclose information on suspected corruption activities. As also stated, elsewhere in this work, the Whistleblower Act is the primary legislation on members of the public making disclosure on various wrongdoings/ offence. As a result, any such disclosures to be made in respect of any suspected crime, in this case corruption related activities, must comply with the provision of the Whistleblowers Act.

The Act provides for category of persons who qualify to make such disclosures.³⁴ They include an employee in respect of an employer³⁵ or another employee³⁶, a person in respect of another person, or an institution.³⁷ Section 2 of the Act states that:

“2. Disclosure of impropriety may be made

(a) by an employee in respect of an employer,

(b) by an employee in respect of another employee, or

(c) by a person in respect of another person, or an institution.”

The Act further provides for persons to whom or institution to which such disclosure of impropriety may be made.³⁸ It provides for disclosures to be made to any one or more of the following:

(a) an employer of the whistleblower; (b) a police officer; (c) the Attorney-General; (d) the Auditor-General; (e) a staff of the Intelligence Agencies; (f) a member of Parliament; (g) the Serious Fraud Office; (h) the Commission on Human Rights and Administrative Justice; (i) the National Media Commission; (j) the Narcotic Control Board; (k) a chief; (l) the head or an elder of the family of the whistleblower; (m) a head of a recognised religious body; (n) a member of a District Assembly; (o) a Minister of State; (p) the Office of the President; (q) the Revenue Agencies Governing Board; or (r) a District Chief Executive.³⁹

³⁴ Section 2, Whistleblower Act, 2006 (Act 720)

³⁵ Ibid Section 2(a)

³⁶ Ibid Section 2(b)

³⁷ Ibid Section 2(c)

³⁸ Ibid Section 3

³⁹ Ibid Section 3(1)

From the above, the Whistleblowers Act strictly provides for who can report improprieties and to whom such reports can be made. Only natural persons are recognized as whistleblowers under Section 2 of the Act as stated above.

Further, disclosures are to be made to specific individuals or institutions that are expressly provided for by the Act. Consequently, information provided by entities other than natural persons, or disclosures made to unauthorized persons and institutions, fall outside the purview of the Act and cannot be officially acted upon.

- **Composition of ORAL in line with the requirement of Whistleblower Act, 2006 (Act 720)?**

As stated above, Section 3 of the Act outlines the persons or institutions to whom disclosures of improprieties can be made, either individually or collectively. A pertinent question is whether the composition of the ORAL team is in line with this provision. The ORAL team is made up of five (5) members which includes, Samuel Okudzeto Ablakwa, the Chairman and Member of Parliament for North Tongu Constituency; Daniel Dormelevo, a former Auditor-General; COP (Rtd) Nathaniel Kofi Boakye, a retired Commissioner of Police; Martin Kpebu, a private legal practitioner and Raymond Archer, an investigative Journalist.⁴⁰

Save for Mr. Ablakwa who qualifies as a person to whom such disclosures of improprieties can be made, it is the contention of the author that the composition of the ORAL team does not meet the requirement of the Act under Section 3. Mr. Boakye who is a retired police officer, cannot be considered to meet the requirement of the Act as he is not in active service. Same applies to Mr. Dormelevo who has previously held the office of the Auditor-General.

- **Procedure after Disclosures have been made**

Section 8(1) of the Whistleblowers Act states that:

“8. (1) Where a disclosure is made to a person specified under section 3, the person shall investigate the matter except that where the person to whom the disclosure is made does not have the capability to undertake the investigation, the person shall refer the disclosure as recorded to the Attorney-General or another body as directed by the Attorney-General for investigation within seven working days after receipt of the disclosure.”

The effect of the above is that disclosures made to a person or an institution specified under the Act, must be investigated by that person or institution. However, where the person or institution to whom the disclosure is made does not have the capability to undertake the investigation, then such person or institution shall refer the disclosure

⁴⁰ Ernest K. Arhinful, ‘Mahama forms 5 – member team to collect public reports on suspected corruption cases’ (www. myjoyonline.com 18 December 2024) < <https://www.myjoyonline.com/mahama-forms-5-member-team-to-collect-public-reports-on-suspected-corruption-cases/> > accessed 12 April 2025

as recorded to the Attorney-General or another body as directed by the Attorney-General for investigation within seven working days after receipt of the disclosure. The key phrase to be noted in the above provision is “*Where a disclosure is made to a person specified under section 3, the person shall investigate ...*”. This phrase reinforces the point made that information received or gathered by an institution or person other than that provided for by the Act, cannot be acted upon for investigation.

On 20th December, 2024, the spokesperson for the then President-Elect Mahama announced that the ORAL team has set up various platforms to gather information on suspected corruption cases. It is difficult to ascertain if the ORAL team complied with the provisions of Section 8(1) of the Whistleblowers Act, to make the necessary reference to the appropriate agency, since it lacked investigative powers. This is because it is not clear when the ORAL team stopped receiving and gathering complaints and disclosures contained in the report. On 10th February 2025, when the Chairman of the team was presenting the Committee’s Report to the President, he stated that the ORAL team had worked for about 53 days.⁴¹ The team was set up on the 18th of December, 2024 and the team subsequently set up channels for receiving complaints on 20th December 2024 as stated above. It is the contention of the author that from the time the team set up the platforms for receiving information to the time it submitted its report to the President, the team had worked (receiving complaints and reviewing same) for fifty-one (51) days.

- **Effect of the scope and mandate of ORAL**

The effect of the scope and mandate of ORAL is that the Team, by soliciting public information on suspected corruption, positions itself as a disclosure-receiving institution that gathers information and evidence to refer to the necessary authority. The provision of Section 3 of the Whistleblower Act is clear and unambiguous. The ORAL team as a committee set up by the then President-Elect does not fall under the Act as an institution to which disclosures ought to be made. Consequently, the ORAL Team cannot act as such an institution as provided by the Act as that will be in direct contravention of the Act.

Secondly, it has been established above that the ORAL team does not have the mandate to receive disclosures of various improprieties as it does not fall within the provisions of the Whistleblowers Act.

- **Confidentiality of Such Disclosures**

The Whistleblowers Act makes provision on how persons and institutions that receive disclosures of impropriety are to act. Among other provisions, it imposes a duty of

⁴¹ TV3 Ghana, ‘ORAL Committee presents report to President Mahama’ (10 February 2025) < <https://www.youtube.com/watch?v=HHG0ornci6M> > accessed 12 April 2025

confidentiality on persons and institutions who receive disclosure while criminalising failing to keep disclosures confidential. Section 6(3) of the Act states that:

Where a person to whom the disclosure is made fails to keep confidential the disclosure, the person commits an offence and is liable on summary conviction to a fine of not less than five hundred penalty units and not more than one thousand penalty units or to a term of imprisonment of not less than two years and not more than four years or to both.

Despite the provisions of the Act mandating persons and institutions receiving such disclosure to keep this confidential, some members have publicly disclosed details obtained during their information gathering. One of these includes a dispute which arose concerning a Cantonment land valued at \$700,000 USD, which was allegedly acquired for only GHS 160,000 by former National Intelligence Bureau (NIB) Director, Nana Atobrah Quaicoe.⁴² ORAL member Martin Kpebu publicly made claims suggesting that Mr. Quaicoe had improperly acquired the land, and added that Mr. Quaicoe had contacted the committee to return the said land.⁴³ However, Mr. Quaicoe, through his legal representatives, denied these allegations.⁴⁴ In response to the denial, Mr. Ablakwa, the chairman of the ORAL committee, through his facebook released lease documents, purportedly intercepted from the Lands Commission, to substantiate the initial claims and refute Mr. Quaicoe's denial.⁴⁵ A question that is worth probing is whether, in line with the provision of Section 6(3), the members of ORAL who have acted contrary to the above provision by making disclosure received by them public will be prosecuted by the Attorney-General? It is again the contention of the author that the members failing to keep disclosures made to them or which have come to their knowledge in the course of their work confidential as well as the failure of the Attorney-General to prosecute these offences, raises credibility issues in respect of the ORAL project.

- **Effect of the Information received by ORAL and the Whistleblowers Act.**

What is the effect of the information received by the ORAL team and the effect of the team referring same to the Attorney-General for investigation and possible prosecution? The answer is simple: any information or disclosures made to the ORAL team cannot be the basis of any investigation or possible prosecution by Attorney-General if the same is referred to his/her office. This lies in the fact that ORAL is not a proper institution to receive disclosures or information of any impropriety. The Team will then be a whistleblower in respect of the information gathered. However,

⁴² SpyDa, 'Former NIB Boss Nana Atobrah caught in a \$700,000 Cantonments Land deal – Okudzeto Ablakwa Unveils Evidence' (www.ghananewsonline.com.gh 12 January 2025) <<https://ghananewsonline.com.gh/former-nib-boss-nana-atobrah-caught-in-a-700000-cantonments-land-deal-okudzeto-ablakwa-unveils-evidence/>>accessed 10 April 2025

⁴³ Ibid

⁴⁴ Joy Online, 'NIB D-G bought state lands at Cantoments for ₵160k – Documents reveal' (www.myjoyonline.com 12 January 2025) < <https://www.myjoyonline.com/nib-d-g-bought-state-lands-at-cantoments-for-%C2%A2160k-documents-reveal/> > accessed 10 April 2025

⁴⁵ Ibid

as is stated elsewhere in this work, the act of whistleblowing is strictly limited to natural persons. The ORAL team not being a natural person cannot make disclosures to any applicable institution in respect of any information received in the purview of the Whistleblowers Act.

The supporters of ORAL argue that the initiative is legitimate, legal and in accordance of the Whistleblowers Act, simply because it is tasked with merely gathering information about applicable improprieties and does not by itself investigate or recover looted state assets. On February 8, 2025, Martin Kpebu, a lawyer and a member of the ORAL team, explained on TV3's "The Key Point" program that the ORAL committee was established due to a power vacuum created during the governmental transition period. He asserted that the then President-Elect needed to address such matters (on looting of state assets) but could not act alone and this necessitated the committee's formation. Kpebu emphasized that the committee's work was conducted in accordance with the Whistleblowers Act and that whistleblowing is part of our culture. He also stated that the **committee was specifically set up to receive complaints and petitions** (emphasis added), allowing the new Attorney-General time to settle into their role while the team organized and gathered information.

However, as established above, this argument is flawed and must not be countenanced as it will lead to acting inconsistent to the provisions of the Whistleblowers Act, the very legislation supporters of ORAL seek to validate the initiative with.

It is the position of the author that, not only is ORAL in the performance and fulfilment of its scope and mandate, illegitimate and contrary to applicable legislation, but it is also redundant in view of the discussion on the legal framework and various investigative and prosecutorial institutions above.

In addition to the point above, the Whistleblowers Act establishes a Whistleblower Reward fund⁴⁶, the object of which is to provide funds for payment of monetary rewards to whistleblowers.⁴⁷ The Act states in Section 24 as follows:

Section 24—Reward on recovery of money

A whistleblower whose disclosure results in the recovery of an amount of money shall be rewarded from the Fund with

(a) ten percent of the amount of money recovered, or

(b) the amount of money that the Attorney-General shall, in consultation with the Inspector General of Police, determine.”

⁴⁶ Section 20, Whistleblower Act, 2006 (Act 720)

⁴⁷ Ibid Section 22

It has been argued above that the ORAL team is not a proper institution to receive disclosures or information of any impropriety and that the ORAL team in effect becomes the whistleblower and the persons making the disclosures. The question that arises in this instance is who will the reward due be paid to, the members of the ORAL team or the unidentified persons who made the disclosures? These gaps created by the implementation of the mandate and scope of the ORAL team supports the contention of the author that the ORAL project is contrary to applicable legislation and also redundant.

Conclusion

Ghana has a comprehensive legal framework for the recovery of looted state assets. There are also several anti-corruption institutions that have the mandate to gather information, investigate and prosecute corruption and corruption-related offences that have led to looting of state assets. To assist with gathering of evidence and information in order to effectively and efficiently investigate and prosecute offenders, the Whistleblowers Act provides for various categories of natural persons to make disclosures by way of information of such impropriety. The Act also provide for such disclosures to be made to specific persons and institutions who may then investigate or make a referral of disclosures to the Attorney-General or the appropriate institution.

ORAL being a committee is not within the purview of the Whistleblowers Act, in respect of persons and institutions that disclosure of improprieties can be made to. Additionally, ORAL is not a natural person and does not fall within the category of persons who can make disclosure of improprieties to the applicable person or institution. As a result, information received by ORAL cannot properly be acted on by way of investigations and possible prosecution by the Attorney-General or any applicable institution to which information is referred. Consequently, ORAL is not legitimate in the context of the provisions of the Whistleblowers Act.



ICC FraudNet
Global Annual Report 2025

Will the Dam Walls Burst? The State of Play in Turning the Tide on Corruption and Fraud in South Africa

**JOHN OXENHAM, MICHAEL-JAMES
CURRIE AND BRANDON COLE**

iccfraudnet.org

ICC |  **FraudNet**



Will the Dam Walls Burst? The State of Play in Turning the Tide on Corruption and Fraud in South Africa

**John Oxenham, Michael-James Currie
and Brandon Cole**

Introduction

Nearly a decade after the height of South Africa's state capture scandal, the promise of a new era of transparency and accountability still hangs in the balance. Although the Zondo Commission exposed the architecture of systemic corruption, the implementation of its recommendations through legislative and regulatory reform has progressed at a glacial pace.¹

Following from our previous contribution to the FraudNet global annual report in respect of the use of non-trial resolutions ('NTR') in complex corruption and fraud cases, this article assesses recent developments in respect of South Africa's anti-corruption and asset recovery landscape by considering three core areas: (i) progress following the Zondo Commission, (ii) South Africa's efforts to address the Financial Action Task Force ('FATF') greylisting, and (iii) compliance with OECD 2021 Anti-Bribery Recommendations.² We focus particularly on developments impacting the detection, evidence gathering, and enforcement of cross-border economic crimes.

¹ Judicial Commission of Inquiry into Allegations of State Capture, Corruption and Fraud in the Public Sector

² OECD, *Recommendation of the Council for Further Combating Bribery of Foreign Public Officials in International Business Transactions*, OECD/LEGAL/0378.

The National Prosecuting Authority (‘NPA’), central to the country’s anti-corruption efforts, remains chronically under-resourced and structurally burdened. Its limited prosecutorial capacity, especially in navigating complex, transnational economic crime cases, continues to hamper efforts to address fraud and corruption.

Despite increasing public awareness and international scrutiny, South Africa’s ability to effectively combat cross-border financial crime remains undermined by fragile institutions and gaps in operational capacity. The need for legislative and regulatory development, strategic enforcement mechanisms, and cross-jurisdictional collaboration has never been more urgent.

Non-Trial Resolutions (‘NTRs’) post-Zondo

One of the positive developments arising from the Zondo Commission was the recommendation to introduce NTR’s into South Africa’s legal framework. This has been identified as a priority for the NPA to assist in reducing the significant backlog of complex cross-border economic crime and corruption cases.

The NPA published a framework for NTR’s titled “*Corporate Alternative Dispute Resolution Policy*” on 2 February 2024, providing clarity on the terms under which NTRs may be pursued. The NTR’s demand that individual wrongdoers be named, and that companies assist the NPA in prosecuting such individuals, ensuring a measure of personal accountability alongside corporate liability.

NTRs have yielded high-profile precedents. In a recent matter, a firm agreed to repay nearly R870 million for its role in state capture-related contracts with Eskom and Transnet, without any formal admission of guilt in a criminal court.³ Similarly, Glencore’s international plea agreement, involving a US\$1.1 billion fine for foreign bribery, demonstrates the potential of NTRs to secure significant penalties while circumventing the delays and complexity of full-scale prosecutions.⁴

The OECD’s Anti-Bribery Recommendations explicitly encourage member states to adopt settlements, deferred prosecution agreements, and other pragmatic tools to address transnational corruption and identified this as a shortcoming vis-à-vis South Africa.⁵

³ See: <https://www.justice.gov/archives/opa/pr/mckinsey-company-africa-pay-over-122m-connectionbribery-south-african-government-officials> Article dated: Thursday, December 5, 2024, first accessed: 18 February 2025.

⁴ See: <https://www.justice.gov/archives/opa/pr/glencore-entered-guilty-pleas-foreign-bribery-and-market-manipulation-schemes> Article dated: Tuesday, May 24, 2024, first accessed 18 February 2025.

⁵ Ibid.

On 20 February 2025, the South African Law Reform Commission published its “Discussion Paper 165” dealing with NTRs.⁶ The discussion paper is largely favourable towards NTRs as a means of dealing with complex multi-jurisdictional corruption cases and makes several recommendations:

- The South African Law Reform Commission (‘SALRC’) should consider whether all modifications to an NTR should be sanctioned by the court;
- The recommendations of the Zondo Commission only apply to corporate and criminal liability, however, it is worth considering extending NTRs in the form of Deferred Prosecution Agreements and Non-Prosecution Agreements to individuals who have committed economic offences;
- Where a director exceeds the scope of their authority by engaging in unlawful conduct, that director may be charged alongside the company with the same offence;
- The SALRC should consider whether legislative amendments to the Criminal Procedure Act should be introduced to allow for deferred prosecutions and non-prosecution agreements.⁷

Comments to the SALRC’s paper closed recently on 30 March 2025, and it is clear that NTRs are a priority for the South African government and likely to be further developed in the coming years.

While the scope of South Africa’s NTR policy may be expanded, it is a positive development that the NPA has formally adopted and utilised the policy in resolving several high-profile and complex cross-border investigations. Critical to obtaining these outcomes was the cooperation between South Africa and several international regulators, including in particular the U.S. Department of Justice.

Regarding the conditions for entry into a NTR, it is suggested that NTRs should be subject to conditions including, but not limited, to the following:

- i. Payment into the criminal asset recovery account of a penalty, determined in terms of sentencing guidelines provided by the legislature, whether in instalments or otherwise.
- ii. Payment of reparations to the victims of the crime, appropriately identified.
- iii. The surrender of profits obtained through committing the offence and any assets purchased with those profits.

⁶ South African Law Reform Commission, Discussion Paper 165 Review of the Criminal Justice system: Non-trial resolutions: Deferred prosecution, alternative dispute resolution and non-prosecution pre-trial process Part A.

⁷ Ibid.

- iv. Full, proactive co-operation in investigations related to the offence committed by the corporation, including offences committed by its directors and employees (as natural persons).
- v. The implementation of a compliance programme or making changes to an existing one related to an organisation's policies and/or employee training, with a focus on preventing, detecting and reporting criminal conduct that may occur within the organisation.
- vi. The institution by the company of disciplinary and, where appropriate, civil action against all directors and employees implicated in offences committed.⁸

Any agreement reached between a company and the NPA must be published, setting out the details of the offence and the basis upon which the matter was deemed suitable for a settlement. Final discretion in these matters' rests with the NPA.⁹

Increased Public Private Collaboration and Strategies

South Africa's primary legislative framework for asset recovery is set out in Chapters 5 and 6 of the Prevention of Organised Crime Act ('POCA'). Chapter 5 is criminal in nature and allows for confiscation and preservation orders in relation to property owned by persons against whom criminal proceedings have been instituted. Chapter 6, on the other hand, allows for obtaining orders based on reasonable grounds to believe that the property concerned are proceeds of unlawful activities.¹⁰

There have been several cases where the NPA has effectively utilised the mechanisms of POCA. Recently, in *National Director of Public Prosecutions v Wood and Others*, the NDPP sought to restrain over R1.6 billion in assets allegedly derived from fraudulent and corrupt contracts awarded by Transnet during the state capture era.¹¹ The Court reaffirmed that restraint orders under Chapter 5 of POCA can be issued even before a conviction, provided there are reasonable grounds to believe that a confiscation order may follow. The High Court's position was challenged but upheld by the Supreme Court of Appeal in June 2024.¹² The case also clarified that benefits under POCA include the gross proceeds of crime and that property held indirectly, such as through trusts, can be subject to restraint.

The judgment confirms that restraint applications must be brought in utmost good faith, but minor or non-material non-disclosures should not derail legitimate State efforts to combat organised corruption through POCA's robust mechanisms.

⁸ Ibid page 33.

⁹ Supra 6 above.

¹⁰ Prevention of Organized Crime Act 121 of 1998.

¹¹ *National Director of Public Prosecutions v Wood, Eric Anthony and Others* Case No: A5021/2021.

¹² *Nybhonyha N O and Others v NDPP* (Case no 972; 973 & 974/22) [2024] ZASCA 113 (16 July 2024).

The challenges to POCA, particularly the effective utilisation of Chapters 5 and 6, mirror the broader systemic issues facing the NPA. The NPA operates in a highly constrained environment marked by institutional fragmentation, chronic under-resourcing, and interdepartmental dysfunction. These difficulties are compounded by legislative ambiguity, low sentencing outcomes, a critical lack of specialised training, and an overburdened prosecutorial workforce.¹³

POCA has in addition attracted constitutional scrutiny, particularly in cases where its civil recovery mechanisms are used following minor regulatory infractions. In *York Timbers v NDPP*, the High Court set aside a confiscation order under section 18 of POCA, highlighting that such proceedings, despite being civil, can have punitive consequences and must be carefully balanced against the right to a fair trial. The court warned against overextending POCA beyond its core purpose of combating organised crime and money laundering, particularly where no demonstrable benefit was derived from the unlawful conduct.¹⁴

The mechanisms provided under POCA, while undoubtedly useful, presuppose that the NPA is able to identify, investigate, and effectively prosecute economic crimes. This remains a significant challenge for the NPA, and unless addressed, it will continue to undermine the full potential and effectiveness of POCA as a tool for asset recovery and economic crime enforcement.

Evidence-Gathering and International Cooperation Tools

In relation to cross-border crimes, key considerations include:

- *Jurisdictional reach*: South African courts can assert authority over assets held abroad through mutual legal assistance mechanisms and cooperation agreements.
- *Legal thresholds*: Freezing foreign bank accounts often requires dual criminality and sufficient evidence under both South African law and the foreign jurisdiction's law.
- *Evidence-gathering mechanisms*: South Africa participates in international treaties such as the UN Convention Against Corruption ('UNCAC')¹⁵, various bilateral Mutual Legal Assistance Treaties ('MLATs'), and engages in informal cooperation through networks like the Egmont Group and Interpol.

These frameworks are essential in tracing and securing offshore assets.

¹³ Kim Thomas, Prosecuting with the Prevention of Organised Crime Act: A Review of South Africa's Anti-Gang Provisions, Research Paper 34, Dullah Omar Institute (November 2022).

¹⁴ *York Timbers Proprietary Limited v National Director of Public Prosecutions* (A626/2013) [2014] ZAGPPHC 641; 2015 (1) SACR 384 (GP); 2015 (3) SA 122 (GP) (22 August 2014).

¹⁵ United Nations, Convention Against Corruption (UNCAC), 2003.

Key Legislative Developments: Prevention and Combating of Corrupt Activities Act 12 of 2004 ('PRECCA') Amendments and Demand-Side Corruption

South Africa has taken significant steps to align its domestic framework with international enforcement regimes like the U.S. Foreign Corrupt Practices Act ('FCPA') and Foreign Extortion Prevention Act ('FEPA').

PRECCA is the principal domestic legislation addressing both demand-side and supply-side corruption in South Africa, and was drafted to align with the UN Convention against Corruption and the AU Convention on Preventing and Combating Corruption.¹⁶ On the demand side, it defines the statutory offence of corruption and sets out specific prohibited acts—such as offering a benefit to influence the awarding of a government contract. On the supply side, it imposes mandatory reporting obligations, with non-compliance carrying serious consequences for both natural and juristic persons.

Previously, PRECCA required, in terms of Section 34, that any person who holds a position of authority and who knows or suspects that any other person has committed an offence, including fraud and corruption, must report such knowledge to the police. A failure to report such a suspicion would constitute a criminal offence.¹⁷

These obligations have been actively utilised in the corporate space, particularly where employees or board members became aware of activities compelling them to file Section 34 reports.

The state has sought to build on the existing framework by introducing section 34A to PRECCA on 3 April 2024. The primary objective of section 34A is to curb demand-side corruption by requiring companies and state-owned entities ('SOE') to implement robust anti-corruption and anti-fraud measures. It establishes a new corporate offence, holding companies and SOEs liable for corrupt activities carried out by individuals within their organisation, unless they can demonstrate that adequate procedures were in place to prevent such conduct.

The amendment provides that a member of a private company or SOE commits an offence if a person associated with them offers, agrees to offer, or gives any form of prohibited gratification with the intention of securing or retaining business.

The amendment is based on Section 7 of the United Kingdom's Bribery Act 2010 which created an offence for commercial organisations failing to prevent bribery. It certainly also builds on the requirements of the FCPA in this regard particularly concerning US based entities operating in South Africa.

¹⁶ See: <https://www.corruptionwatch.org.za/corruption-and-the-law-in-south-africa-part-two/> First accessed: Thursday, 6 March 2025.

¹⁷ Section 34 of the Prevention and Combating of Corrupt Activities Act 12 of 2004.

When viewed in the broader context of the state's legislative and policy reforms to combat corruption and fraud, the recent amendments to PRECCA align closely with the objectives of NTR's. Enhanced reporting obligations under PRECCA are likely to expose additional targets for enforcement, reinforcing the utility of NTRs as a tool for accountability. Other legislative reforms aimed at addressing the FATF's concerns and facilitating South Africa's removal from the grey list, such as amendments to the Companies Act and the introduction of Ultimate Beneficial Ownership ('UBO') declarations, further support this enforcement-oriented approach by promoting greater corporate transparency.

Practical Challenges Facing Anti-Corruption Efforts in South Africa

Even when authorities are able to make substantial headway on certain cases, the fragility of the enforcement landscape is exposed through the violence and intimidation faced by whistleblowers. The assassination of Babita Deokaran, a senior Gauteng health official¹⁸, and the murders of liquidators Cloete and Thomas Murray¹⁹, are stark reminders of the personal risks faced by individuals exposing serious fraud and corruption.

Until South Africa strengthens the structural independence of its anti-corruption institutions, ensures adequate protection for witnesses and whistleblowers, and insulates enforcement bodies from political reprisal, its capacity to hold the powerful accountable will remain severely compromised.

There have been positive regulatory and legislative changes. South Africa's placement on the FATF grey list in early 2023 triggered a wave of regulatory and legislative reforms aimed at addressing strategic deficiencies in its anti-money laundering and counter-terrorist financing regimes.²⁰ However, challenges persist, particularly the need to increase prosecutions for money laundering and terrorist financing offences. Given the NPA's resource constraints and political pressures, this gap poses a significant risk to South Africa's efforts to secure removal from the FATF grey list.

The establishment of a beneficial ownership register is another promising development designed to increase transparency around the true owners of corporate and trust structures.²¹

¹⁸ See: <https://www.oua.co.za/newsletter/aug22/babitadeokaran> Article dated: March 27, 2023, first accessed: Friday April 25, 2025.

¹⁹ See: <https://turnaroundtalk.co.za/special-features-archived/final-case/> First accessed: Friday April 25, 2025 April 25, 2025

²⁰ Financial Action Task Force (FATF), "Jurisdictions under Increased Monitoring — South Africa," February 2023.

²¹ See: <https://support.infodocs.co.za/en/article/everything-you-need-to-know-about-beneficial-ownership-as-of-march-2025-1u4q75o/> Article dated: March 25, 2025, first accessed: April 25, 2025.

Conclusion

South Africa's commitment to combating fraud and corruption faces a critical juncture. While significant progress has been made in addressing technical compliance benchmarks required by the FATF, structural weaknesses within key institutions, such as the National Prosecuting Authority, the Hawks, and the broader Chapter 9 framework, continue to undermine effective enforcement.

Unless systemic vulnerabilities, including resource constraints, political pressures, and operational independence, are addressed in a meaningful and sustained way, South Africa's efforts to restore global confidence and secure removal from the FATF grey list may be severely compromised. More fundamentally, the ability of the country to position itself as a credible international partner in the fight against fraud and corruption depends on rebuilding robust, independent enforcement mechanisms.

Renewed political will, strategic reform, and meaningful investment in institutional resilience are urgently needed if South Africa is to make real progress in combating corruption. Political will remains the key barrier, yet with mounting pressure on the ruling party (the African National Congress), who for the first time lost its outright majority in the 2024 elections, the window for decisive action is narrowing. It is now or never for South Africa to get it right.



ICC FraudNet
Global Annual Report 2025

Corporate Transparency in Anti-Money Laundering: Where are we?

DR DOMINIC THOMAS-JAMES



iccfraudnet.org

ICC  **FraudNet**



Corporate Transparency In AML – Where Are We?

**Dr Dominic Thomas-James
Yale University Global Justice Program,
Goldsmith Chambers and ICC FraudNet**

Introduction

Ever since the publications of law firm data from the offshore world in what is known as the Panama and Paradise papers, among others, the anti-money laundering (‘AML’) regime has seen significant developments in the area of corporate transparency of ultimate beneficial ownership information (‘UBO information’). For some time in the wake of these leaks, given the international reverberations and spotlight shown on the world of offshore jurisdictions and their incorporations sectors, momentum was geared towards free and public access to such information. Given the accepted relationship between anonymous corporate vehicles and the opportunity for illicit activity, the argument for public registries seemed difficult to argue against.

Indeed, the UK has provided access to its Persons with Significant Control Register for free and to any member of the general public for nearly a decade, in which controllers of more than 25% of the voting rights of an entity on the register would have to report their UBO information. Elsewhere, momentum has been firmly in this direction – with an example being seen in the European Union’s Fifth AML Directive (2018/843), which required UBO information to be made available by each member state to any member of the general public. In other words, going far beyond legitimate interest access.

In 2018, in the wake of the aforesaid data leaks, the UK Parliament enacted section 51 Sanctions and Anti-Money Laundering Act which, given that many UK Overseas Territories were mentioned in the leaks, compelled these jurisdictions to implement public registers. Several of them already had functioning central registers, but not publicly accessible. Despite what is, effectively, a legislative ultimatum from the UK – this effort is still ongoing at the time of writing. In June 2025, for example, the British Virgin Islands published a policy outlining legitimate interest access to UBO information.¹

In the context of transparency efforts on UBO information, I have long argued that too much focus has been put on the optics and purported benefits of transparent registers, at the expense of greater emphasis on the mechanics of a properly functioning register. The ‘junk information, junk information out’ argument is not new – but has plagued the UK’s register to the extent urgent reforms including better use of verification technology, are well underway. The argument has, however, long been trumped by the purported benefits of transparency which are often difficult to argue against given the international weight placed on events like the Panama papers and corresponding transparency efforts thereafter. However, developments seen recently at both the EU and US levels have shone an increasingly bright light on fundamental safeguards and the limits of transparency, which now appears to be at the forefront of the UBO information debate. These, of course, pertain to concerns about privacy, data protection and, in the case of the US situation, the issue of burdensome regulation on domestic entities.

Discussion

Some elements of the AML apparatus, as a primary response to financial crime, appear straightforward and perhaps less controversial. For example, the criminalisation of money laundering² or the implementation of a banking supervisory framework which raises red-flags if certain banking transactions, destinations or clients raise suspicion or require enhanced due diligence.³ However, the question of an appropriate UBO information standard remains controversial, as is the extent to which it should be held on a register, or, importantly, to whom that information should be made available and in what circumstances, is a complex issue. There is divergence of opinion on whether it should be freely and publicly accessible, as it is in the UK, or only accessible to those with a legitimate interest (and, in which case, to whom that relates), or only to competent investigative authorities and law enforcement. While certain Directives like the EU’s 5th AML Directive had initially mandated access to any member of the general public, interestingly, the Financial Action Task Force (‘FATF’) Recommendation 24,

¹ See, Government of the Virgin Islands, Press Release: BVI Publishes Policy on Legitimate Interest Access to Beneficial Ownership Register, 23 June 2025, available at: <https://bvi.gov.vg/media-centre/bvi-publishes-policy-legitimate-interest-access-beneficial-ownership-register> (accessed 25 Jul 2025).

² Financial Action Task Force Recommendation 1.

³ Ibid, Recommendation 13.

even in its most recent review and guidance note,⁴ declines to mandate an approach, instead indicating various pathways toward potential compliance.

What is particularly concerning with the UBO debate is that there has for some time existed the view that there is something inherently wrong about members of the public not having access to company UBO information. In justifying public access and the imposition of this on UK Overseas Territories under section 51 Sanctions and Anti-Money Laundering Act, the Rt. Hon. Andrew Mitchell MP stated: “The [UK Overseas] territories may well allow access to law and order agencies, within an hour in the case of terrorism, through closed registers, but that does not allow civil society – charities, NGOs and the media – to expose them to the sort of scrutiny that the Paradise and Panama papers did”.⁵

Corporate transparency arguments have long been predicated on the assumption that it is not satisfactory that UBO information is only available to investigative authorities, and not the general public, the media or NGOs etc. Through my research, I have yet to see any impact assessments which posit, or conclude, that centrally held registers – such as those accessible to only competent investigative authorities (which may well make a country compliant with FATF Recommendation 24) are any less effective than public ones in terms of investigating and interdicting financial crime. The UK is presently making significant reforms to its registry,⁶ but as background to this, in 2022 the UK Government in a White Paper astonishingly acknowledged that Companies House has become “a passive recipient of data”⁷ and that it needs to become a more active gatekeeper.

Therefore, does this – i.e. not being a passive recipient of data – need to be the first step when measuring the likely effectiveness of a UBO register? If the registrar is equipped with necessary infrastructure through which information can be properly verified using technology that is widely available in other avenues of financial transacting, and that any errors can be properly rectified and eradicated, then might we start to see more of an effective register that is a useful resource for law enforcement purposes, a tool for due diligence and risk management – regardless of whether that information is publicly accessible or only government-held.

As noted above, transparency itself may well sound positive and perhaps difficult to argue against since events like the Panama papers. The notion of shining light on that which is dark is an undeniably powerful argument. However, transparency in the context of UBO information should not be viewed in absolutist terms. Dichotomous

⁴ See, Financial Action Task Force Guidance on Beneficial Ownership of Legal Persons, March 2023, available at: <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Beneficial-Ownership-Legal-Persons.pdf.coredownload.pdf> (accessed 10 March 2025).

⁵ HC Deb, 1.5.2018, Vol 640, Col 203, Rt. Hon. Andrew Mitchell MP.

⁶ Companies House is the UK Authority that maintains the companies register, including information on Persons with Significant Control.

⁷ See: White Paper, Dept for Business, Energy and Industrial Strategy, ‘Corporate Transparency and Register Reform’, (HMSO, 2022), p12.

thinking on UBO transparency risks missing the wood for the trees and rests on overly simplistic ground in terms of how transparency may operate for the above purposes, and what its objectives may be. Transparency itself in this context *can* be a tool, but should not be simply a virtue. Therein lies the problem with UBO information - given its status relative to fundamental legal safeguards. It is important to maintain a distinction between information that is properly ‘of interest’ for some substantive reason, and information which is simply ‘interesting’ out of curiosity – particularly in the face of privacy considerations that have re-entered the debate as legitimate concerns. Like any tool which is predicated on receiving or maintaining personal information, there needs to be checks and balances.

This question of unfettered public access at the forefront of the transparency movement was recently subject to European jurisprudence in the matter of *WM and Sovim SA v Luxembourg Business Registers* [2022].⁸ In this case, the court held that the public accessibility requirements of UBO registers under the provisions of the 5th EU AML Directive, risked undermining fundamental rights under the Charter of Fundamental Rights of the European Union – i.e. Article 7 – the right to respect for private and family life, and the Article 8 – the right to the protection of personal data. In the wake of this decision, overnight many registers in the Community that were previously public in compliance with the 5th AML Directive, were removed and this issue continues to be a matter of ongoing development at the European level.

If things were not confusing enough on the UBO issue, most recently the United States has become an outlier in what some critics are saying will “open the floodgates to dirty money”.⁹ In March 2025, the US Treasury Department announced it was suspending enforcement of the Corporate Transparency Act against US citizens and domestic reporting companies, noting: “it will not enforce any penalties or fines associated with the beneficial ownership information reporting rule under the existing regulatory deadlines [and] it will further not enforce any penalties or fines against U.S. citizens or domestic reporting companies or their beneficial owners after the forthcoming rule changes take effect”.¹⁰ It announced that the Department will propose narrowing the scope of the rule only to foreign reporting companies. It appears that the underlining philosophy of this move, which clearly contrasts with transparency efforts in recent years including the CTA coming into force in 2024, takes aim at supporting “hard-working American taxpayers and small businesses” and rein-in “burdensome regulations, in particular for small businesses”.¹¹ As such, the landscape is anything but clear – which certainly leads to the conclusion that the question of the appropriateness, or otherwise, of so-called international AML/CFT standards requires further thought.

⁸ (C-37/20 and C-601/20) EU: C:2022:912; [2023] Bus. L.R. 611.

⁹ See, for example, FACT Coalition Press Release, available at: <https://thefactcoalition.org/treasury-reopens-the-floodgates-to-dirty-money-cta/> (accessed 20 March 2025).

¹⁰ US Department of the Treasury, Press Release, 2 March 2025, available at: <https://home.treasury.gov/news/press-releases/sb0038> (accessed 10 March 2025).

¹¹ Ibid.

Conclusion

On UBO information, and the question of registers, it seems as though the world is as untethered now as it has ever been. The FATF, who have long been the international standard bearer on AML/CFT as a primary response to financial crime, stops short of mandating an approach on UBO information and highlights that there can be various routes to compliance. Meanwhile, the UK is phasing in register reforms to make it a more active gatekeeper of public information to enhance its now decade-long publicly accessible register. Elsewhere, close neighbours have been seen to take their public UBO registers offline and there are concerns about fundamental legal safeguards and Charter rights. Across the pond, there is pushback from even a requirement for domestic company reporting UBO information to a central register and concerns raised about UBO information and its burdensome regulatory nature. In other jurisdictions, like the BVI, we see a push towards legitimate interest access. What this state of confusion and disparity leads to is not an answer on what the correct standard ought to be on UBO registers; but rather demonstrates the challenges that a one-size-fits-all approach to some key elements of global AML apparatus presents. This space is dynamic and evolving, but it will be interesting to see from whom others take their manners and what the approach(es) will be to this complex and controversial issue.



ICC FraudNet
Global Annual Report 2025

Equitable Liens and Fraud

WILLIAM FOTHERBY



Equitable Liens and Fraud

William Fotherby
Meredith Connell

Introduction

A modest equitable-lien renaissance is afoot in New Zealand. Several recent cases have examined them in the insolvency context. This attention has left the door open to a wider role for this often-overlooked proprietary remedy. This article examines this recent case law before exploring the remedy's potential as an instrument against fraud. It builds on the work on equitable remedies and fraud in our last ICC FraudNet Global Annual Report contribution, which analysed the remedy of appointing a receiver to a trust.¹

The Nature and Origins of Equitable Liens

The origins and scope of equitable liens are uncertain. There seem to be three competing theories as to origin. The first is 19th Century decisions in the Court of Chancery. The second is it sprung from common law lien principles from around this time that developed in response to changing mercantile needs. The third is that an old ancestor of the remedy is the Roman *hypotheca*—the pledge of an item without the need for physical transfer—which of course is the ancestor of the mortgage as well.²

¹ W Fotherby and D Muratbegovic, 'Appointing a Receiver to a Trust in New Zealand' in *ICC FraudNet, Global Annual Report 2024: Asset Recovery – Onshore and Offshore* (ICC FraudNet 2024) 46–49.

² See F Burns, "The Equitable Lien Rediscovered: A Remedy for the 21st Century" (2002) 25(1) UNSW Law Journal 1 at 6 –7.

As for when they arise, the Court of Appeal noted in *Francis* (infra) that one commentator had described the circumstances in which they may arise as “something of a themeless rag bag”.³ So, it is easier to start with what they are not.

A lien at common law entitles a creditor to retain a debtor’s goods in its possession until a debt is paid. It may arise by virtue of common law right, by agreement or by statute. A well-known example is probably the repairer’s lien: repairers may retain goods (such as a car) that they have repaired until the bill for that repair is paid. Another well-known example is the solicitor’s lien: the right of solicitors to resist an instruction to transfer their files pending payment of their fees.⁴ Common-law liens depend on the creditor having possession of the property subject to lien, which is a limiting factor. An equitable lien is different because it exists “quite irrespective of possession”.⁵ And, whereas a common-law lien only gives the right to detain property until payment, an equitable lien typically gives its holder a right to judicial sale of property, or for an order for payment out of a fund.⁶ It is imposed by equity because of the nature of the relationship between the parties or from a course of conduct. While it does not give the holder the right to a transfer of the property or to use it, it is nonetheless a proprietary right, will survive the insolvency of the owner,⁷ and in principle allows the lien-holder to exercise rights in relation to that property such that they may exercise their right of judicial sale. Examples of established equitable liens include:

- a vendor’s lien over land to secure payment of the purchase price where transfer occurs before payment (although now abolished in New Zealand by statute);⁸
- (conversely), a purchaser’s lien over land to secure repayment of the purchase price if the agreement terminates before transfer;⁹
- the liens of trustees over trust assets for expenses in administering the trust or estate, and other similar “salvage” type cases;¹⁰ and
- a beneficiary’s equitable lien over the assets acquired by a trustee who has misappropriated trust funds.¹¹

As mentioned above, the requirements for an equitable lien to arise defy characterisation, or at the very least are heavily circumstance dependent. It is easy enough, at one end of the spectrum, to find comments that they are founded on general considerations of justice, or even a “fiction” in order to achieve it.¹² At the

³ D Waters “Where is **equity** going?” (1988) 18 WALR 3 at 24.

⁴ Roger Fenton, *Garrow and Fenton’s Law of Personal Property in New Zealand* (7th ed, LexisNexis, Wellington, 2010) vol 1 at 645.

⁵ Halsbury’s Laws of England, “Equitable Lien” in *Lien* vol 68 (5th ed, LexisNexis, London, 2021) para 3.

⁶ Ibid.

⁷ A to Z of New Zealand Law (online ed, Thomson Reuters) at [51.10.4].

⁸ Noted in *Francis v Gross* [2024] NZCA 528 at [66].

⁹ Ibid.

¹⁰ Fenton, above n 4, at 668.

¹¹ *As in Foskett v McKeown* [2001] 1 AC 102.

¹² *Wytches v Lee* (1855) 3 Drew 396; *Rose v Watson* (1864) 10 HL Cas 672 at 681; *Whitbread & Co Ltd v Watt* [1902] 1 Ch 835 at 840.

other end is a decision of Deane J of the High Court of Australia, who carefully—and in terms of what would be sufficient but not essential—enumerated when an equitable lien would arise between parties to a contractual relationship (in the context of the modular housing that purchasers had paid for but not received):¹³

- (a) indebtedness by the owner of the property to the other party arising from a payment in relation to the acquisition of the property or of an expense incurred in relation to it;
- (b) that the property be identified and appropriated to the performance of the contract; and
- (c) the relationship between the indebtedness and the property being such that the owner would be acting unconscientiously or unfairly if they were to dispose of the property without liability having been discharged.

Burns puts this decision at the heart of a general rearticulation and expansion of equitable remedies that the High Court of Australia undertook in the late 20th century—as a response to evolving commercial needs—and Justice Deane’s judgment itself as leaving open the situations that could trigger an equitable lien, while articulating broad but meaningful standards for when it would arise.¹⁴ And it is the same context of modular housing in which the issue has arisen recently in New Zealand.

Francis v Gross

In a forerunning case, *Maginness & Booth v Tiny Town Projects Ltd (in liq)*,¹⁵ purchasers had advanced funds for modular home construction by Tiny Town Projects, which subsequently entered liquidation with homes in various stages of completion. Justice Venning determined that these purchasers held an equitable lien over the partially completed homes to the extent of their payments. A key factor was the distinct identity of the tiny homes for specific purchasers and their limited marketability elsewhere. The Court deemed equitable intervention appropriate to uphold such a lien, effectively classifying the purchasers as secured creditors over those specific assets.

This decision found initial application soon after in *Francis v Gross*,¹⁶ where the High Court applied *Tiny Town* principles to similar facts. On appeal, however, the Court of Appeal disagreed, finding that the purchasers of the partly constructed modular buildings did not possess an equitable lien. The Court’s reasoning was largely that recognizing an equitable lien in this type of case would disrupt the established priority regime under the Personal Property Securities Act 1999 (‘PPSA’) and insolvency legislation. The Court emphasized Parliament’s creation of a comprehensive framework for creditor priority, cautioning against judicial creation of equitable

¹³ *Hewett v Court* [1983] 149 CLR 639 at 668.

¹⁴ Burns, above n 2, at 15.

¹⁵ *Maginness & Booth v Tiny Town Projects Ltd (in liq)* [2023] NZHC 494.

¹⁶ *Francis v Gross* [2023] NZHC 1107.

remedies that undermined this framework.¹⁷ It was also concerned that granting an equitable lien to purchasers whose homes had been started, but not to those who had paid deposits but work had yet to begin, would create an unjustified distinction among unsecured creditors.

Essentially, when looking to Deane J's three criteria listed above, the Court concluded that statutory priorities upon insolvency imposed their own type of fairness. The owner of the property—here the liquidator—would not be acting unfairly by following them.¹⁸ These priorities supplied the negative answer to unconscionability.

The Court also took the opportunity to canvass briefly another form of equitable lien—the liquidators' lien over funds identified, protected and realized.¹⁹

So, although the purchasers' claims were ultimately unsuccessful before the Court of Appeal, the detailed discussion of principle in *Francis v Gross* has put equitable liens back on the remedial map. The final section of this article discusses how they might be used to assist cases of fraud.

The Equitable Lien and Fraud

We have already encountered one example of an equitable lien applying in a case of fraud. In *Foskett v McKeown*—an argument about entitlements to a life-insurance pay out after a defaulting trustee used trust funds to pay the premiums—Lord Millet's majority judgment noted that where a trustee misappropriated trust property and used it to acquire other property for their own benefit, the beneficiary was entitled *either* to assert his beneficial ownership of the proceeds *or* to bring a personal claim against the trustee (for breach of trust) and enforce an equitable lien on the proceeds to have the trust funds returned. The beneficiary could normally exercise the option in the way most advantageous to them.²⁰ Where the value of the proceeds has gone down, a personal claim, enforced by way of lien, may well be the preference. The lien would extend to covering interest and costs.

Another possible use case was discussed by no less than Justice Bill Gummow, in a 1993 case note in the Law Quarterly Review.²¹ In the case noted, *Lord Napier and Ettrick v. Hunter*,²² a managing agent had failed to obtain adequate reinsurance for an insurance syndicate relating to certain asbestos claims. The syndicate had gone off and obtained general reinsurance with some "Stop Loss Insurers", but claims on this reinsurance did not completely cover the syndicate's losses. So, the syndicate sued the managing

¹⁷ At [150].

¹⁸ At [96].

¹⁹ At [154].

²⁰ *Foskett v McKeown* [2001] 1 AC 102 at 130–131. Most famously, in these passages, Lord Millet abolished the rule where there was a mixed substitution—involving a purchase with mixed trust funds and non-trust funds—the beneficiary was confined to a lien.

²¹ W Gummow "Names and Equitable Liens" (1993) 109 LQR 159

²² *Napier v Hunter* [1993] AC 713.

agent for negligence and breach of duty, a claim that settled for £116 million. The question in *Napier* was whether the Stop Loss Insurers could claim against these settlement proceeds, still held by the syndicate's solicitors, for the amounts they had paid out to the syndicate.

The House of Lords said, "yes": The Stop Loss Insurers had a proprietary right in the proceeds supported by an equitable lien. The lien would be enforceable against such proceeds so long as it was traceable and had not been acquired by a bona fide purchaser for value without notice. The lien arose either from an implied term in the contract of insurance or to protect the utility of the insurer's right of subrogation by protecting the ability to claim out of damages recovered from the wrongdoer.²³

In his note, Justice Gummow suggested that this decision might lead to greater attention to the equitable lien in those jurisdictions (such as New Zealand) that were willing to consider the imposition of a remedial constructive trust. This suggestion arose because there may be cases where while "the full panoply of trust may exceed the needs of the particular case" the less intrusive imposition of a lien may allow a Court to give effect to the equity established by the successful party,²⁴ particularly where the obligations associated with trusteeship would be incongruous or inappropriate in the circumstances. In essence, Justice Gummow suggests that because equitable liens involve a less intrusive imposition on property rights compared to, for example, a constructive trust, they may be a more appropriate remedy in situations where equity intervenes to rectify unconscionable conduct.

Indeed, the most notable case of a remedial constructive trust in New Zealand, Justice Glazebrook's decision in *Commonwealth Reserves I v Chodar*,²⁵ arose from a case where the victims of a fraudulent scheme could not show that the only assets available to claim against (the yacht *Lady Godiva* and a house) had been purchased with trust money, or held in the context of a fiduciary relationship. Nonetheless, the fraudsters had transferred funds to the defendants who purchased the yacht and property, and these defendants had knowledge of the fraud and the fraudsters' intent to defeat the plaintiffs' claim. Justice Glazebrook held that a remedial constructive trust is appropriate only when other remedies are inadequate, which she found to be the case there.²⁶ The Court thus vested legal and beneficial ownership in the vessel and property in the plaintiffs.²⁷

New Zealand courts use remedial constructive trusts sparingly due to concerns about their discretionary nature and potential to disrupt existing proprietary rights, as suggested by Nourse LJ in the English decision of *Re Polly Peck International (No 2)*,

²³ Gummow, above n 21, at 162.

²⁴ Ibid at 163.

²⁵ *Commonwealth Reserves I v Chodar* [2001] 2 NZLR 374.

²⁶ At [61].

²⁷ At [63].

which was generally hostile to the idea.²⁸ *Chodar* itself drew criticism for relying heavily on unconscionability without sufficient justification and for treating the interests of third parties as a defence rather than a factor in the initial determination of appropriateness.²⁹

An equitable lien offers a way to avoid some of these difficulties. Justice Deane's third criterion provides guidance for establishing a lien, even outside of contract: whether "the owner would be acting unconscientiously or unfairly if they were to dispose of the property without liability having been discharged". As established in *Francis v Goss*, the court's analysis of unconscionability includes considering the interplay with statute, particularly the rights of third parties in insolvency. While a flexible remedy, the Court will not impose a lien if it conflicts with statutory insolvency rules. The Privy Council's decision in *re Goldcorp* illustrates this point:³⁰ even in cases of misappropriation, a court may decline to impose a lien if it would give one class of claimants an unfair advantage over others. One further point is that a remedy allowing a judicial sale (and giving the plaintiff sufficient proprietary rights to exercise this remedy) does seem to offer a more orderly realization of assets than the vesting of title in the plaintiffs that occurred in *Chodar*.

A final point on equitable liens and fraud arises from the liquidators' lien discussed in *Francis v Goss*. It is generally established where an agent realizes funds on behalf of a body of creditors. It seems clear that someone who realizes funds on behalf of fraud victims would have a strong claim for the costs of realization as well, secured by such a lien.

²⁸ *Re Polly Peck International* (No 2) [1998] 3 All ER 812 (CA) (at p 831).

²⁹ Dr A Butler, *Equity and Trusts in New Zealand* (Westlaw, Online Looseleaf Ed) at [13.3].

³⁰ *In re Goldcorp Exchange Ltd* [1995] 1 AC 74 (PC) at 110–111.

ICC FraudNet
Global Annual Report 2025

Part VI: Practical Perspectives

iccfraudnet.org





ICC FraudNet
Global Annual Report 2025

Should you Agree to Arbitrate in the United States? An Overview and Practical Considerations

**JOE WIELEBINSKI AND
MATTHIAS KLEINSASSER**



Should you Agree to Arbitrate in the United States? An Overview and Practical Considerations

**Joe Wielebinski
and Matthias Kleinsasser, Winstead**

Arbitration as a dispute resolution process continues to grow in popularity in the United States ('U.S.'), particularly with respect to international matters. This article first provides an overview of the arbitration process in the U.S., including statutory authority, drafting arbitration clauses, and the arbitration proceeding. This article concludes with a summary of the pros and cons of arbitration in the U.S., with particular emphasis on issues such as cost and confidentiality.

I. Introduction

Arbitration is a dispute resolution process by which parties agree to have disputes adjudicated by one or more individuals (arbitrators), rather than through the court system. Over the preceding decades, the popularity of arbitration has increased, both in the U.S. and with respect to international matters.

The scope of this article is two-fold: First, we provide a general overview of the arbitration process in the U.S., from statutory authority, to crafting the arbitration clause, to the arbitration proceeding. Second, we identify the pros and cons of arbitration in the U.S., focusing on issues such as cost, confidentiality, and third-party discovery.

II. An Overview of the Arbitration Process in the United States

1. Federal and State Arbitration Statutes

Both federal law and state law in the U.S. permit arbitration as a dispute resolution process. The Federal Arbitration Act (“FAA”) applies to agreements involving interstate commerce, which encompasses most business contracts.¹ There are numerous state statutes available with their own jurisdictional provisions. For example, the Texas Arbitration Act can be incorporated into any contract governed by, or invoking, Texas law.² This means that parties negotiating a contract will typically have at least two statutes available to govern arbitration: the FAA and whatever state arbitration statute(s) are available based on the law applicable to the contract.

The FAA and state statutes generally govern issues such as the enforceability of arbitration agreements, compelling arbitration and staying court litigation, appointing arbitrators, compelling attendance of witnesses, and confirmation of arbitration awards.³ It is common for parties not to expressly reference either the FAA or a state statute in their arbitration clause. Omitting a reference to the FAA does not necessarily make the FAA inapplicable. On the contrary, the FAA applies to almost any contract involving economic activity in interstate commerce unless the agreement expressly states that arbitration shall be governed by a state statute.⁴ Nor does the applicability of the FAA mean that a state arbitration statute cannot also apply to the agreement. Typically, both the FAA and a state statute will be applicable. The FAA preempts the state statute only if the state statute’s provisions are inconsistent with the FAA or would subvert enforcement of an agreement otherwise enforceable under the FAA.⁵ If the parties expressly select only the FAA or a state arbitration statute in their agreement, that designation will be upheld provided that the jurisdictional requirements for the selected statute are satisfied (e.g., in the case of the FAA, that the agreement is connected to interstate economic activity).⁶

In determining whether to exclusively select the FAA or a state arbitration statute, it is worth researching not only the jurisdictional requirements of each potential choice, but also the differences between them. State arbitration statutes sometimes differ from the FAA in ways that can be advantageous or disadvantageous, depending on a party’s

¹ 9 U.S.C. §§ 2 *et seq.*

² Tex. Civ. Prac. & Rem. Code §§ 171.001 *et seq.*

³ *See, e.g.*, 9 U.S.C. §§ 2-5, 7, 9-11.

⁴ 9 U.S.C. § 1 includes an exception from the scope of the FAA for employment contracts of seamen, railroad employees, and other classes of workers engaged in foreign or interstate commerce.

⁵ *See, e.g., Scott v. Grim*, 2024 Tex. App. LEXIS 7472, *5 (Tex. App.—Oct. 21, 2024, no pet.).

⁶ *See, e.g., Mammoth Energy Servs. v. Summers*, 2025 Tex. App. LEXIS 151, *11 (Tex. App.—Texarkana Jan. 16, 2025, no pet.) (“Where an arbitration agreement expressly states that the FAA governs, appellate courts will uphold that designation.”); *Tex. Reit, LLC v. Mokaram-Latif W. Loop, Ltd.*, 2022 Tex. App. LEXIS 8871, *4 (Tex. App.—Houston [14th Dist.] Dec. 6, 2022, pet. denied) (mem. op) (citing *Nafta Traders*, 339 S.W.3d at 97 n.64 (“As the court of appeals noted, the parties have not disputed the applicability of the TAA to their agreement. The TAA and the FAA may both be applicable to an agreement, absent the parties’ choice of one or the other.”))).

goals. A good example is the expanded judicial review of an arbitration award permitted by the Texas Arbitration Act. After an award is issued by the arbitrator, the prevailing party will seek confirmation of the award in a court of appropriate jurisdiction. Once the award is confirmed, it becomes an enforceable judgment and the prevailing party can seek to satisfy the judgment with the losing party's assets. Confirmation of the award can be challenged, but the bases for doing so are very limited under the FAA and most state statutes. The grounds for setting aside or modifying an arbitration award under the FAA are limited to the bases set forth in Sections 9-11 of the FAA.⁷ Under the Texas Arbitration Act, however, parties can contract for expanded judicial review provided they use clear language in doing so.⁸ This is a significant difference from the scope of review permitted under the FAA. A party concerned about unfavorable arbitrator decisions could select the Texas Arbitration Act as the exclusive statute governing arbitration and include additional bases for review in the arbitration clause (provided the agreement is governed by, or otherwise invokes, Texas law).

2. The Arbitration Clause

At its core, arbitration is a creature of contract. In other words, the ability of a party to demand that a dispute be sent to arbitration rather than litigated in a court depends on whether the matter is within the scope of disputes encompassed by the parties' arbitration clause. The scope of the arbitration clause can also determine the number of arbitrators, the applicable arbitration service provider, the extent of discovery, and numerous other issues.

Because claims are generally arbitrable only if they fall within the scope of the arbitration clause, careful drafting of the arbitration clause is paramount.⁹ A clause stating that any claim "related to" the parties' agreement must be arbitrated, whether arising in contract, tort, or other legal theory, is likely to encompass almost any claim arising as a result of the parties' business relationship. An arbitration clause stating that any claim "arising under the parties' agreement" might be held to encompass only claims involving a breach or interpretation of the contract and likely would not include tort or restitution claims. Parties should ensure that the clause is drafted to include all claims they wish to arbitrate, and should expressly exclude any claims they do not wish to arbitrate (e.g., tort claims).

⁷ *Hall St. Assocs., LLC v. Mattel, Inc.*, 552 U.S. 576, 588 (2008).

⁸ *Forest Oil Corp. v. El Rucio Land & Cattle Co.*, 518 S.W.3d 422, 432 (Tex. 2017).

⁹ A discussion of defenses to a demand for arbitration—e.g., waiver of the right to compel arbitration through excessive delay in making a demand—is beyond the scope of this article. *See, e.g., Morgan v. Sundance, Inc.*, 596 U.S. 411 (2022) (discussing waiver). Also beyond the scope is a discussion regarding how non-signatories to an arbitration agreement may be compelled to arbitrate. *See, e.g., Zurich Am. Ins. Co. v. Watts Indus.*, 417 F.3d 682, 687 (7th Cir. 2005) (discussing the theory of direct benefits estoppel, under which a non-signatory can be required to arbitrate).

A well-drafted arbitration clause should address any issues the parties view as important, should a dispute ensue. Here are some issues that are commonly included in an arbitration clause:

- What claims are included (or excluded) from arbitration?
- The preferred arbitration service provider (e.g., American Arbitration Association, JAMS).
- The number of arbitrators: having three arbitrators minimizes the risk that a rogue arbitrator makes a poor decision, but also significantly increases cost.¹⁰
- Whether an arbitrator may grant equitable or declaratory relief, and whether a party may seek equitable relief on an emergency basis in a court of law.¹¹
- Whether the arbitrator may rule on his own jurisdiction to determine if a claim is arbitrable (see Section II.3 *infra*).
- Permitted discovery methods (e.g., document production requests, interrogatories, depositions) and any limitations as to the number of requests, depositions, etc.
- The court having jurisdiction to confirm an arbitration award.
- Whether a confirmed arbitration award can be appealed.

3. The Arbitrator's Jurisdiction – Who Determines It?

The U.S. Supreme Court has recognized three layers of arbitration disputes: (1) merits—who prevails in the underlying dispute between the parties based on relevant law and facts; (2) arbitrability—did the parties agree to arbitrate the merits of their dispute; and (3) who decides arbitrability—is the arbitrability of a dispute determined by a court or the arbitrator?¹² The U.S. Supreme Court has emphasized that the third question, like the second, is a matter of consent. “Just as the arbitrability of the merits of a dispute depends upon whether the parties agreed to arbitrate that dispute, so the question ‘who has the primary power to decide arbitrability’ turns upon what the parties agreed about *that* matter.”¹³

In short, it is possible for an arbitrator to rule on his/her own jurisdiction to decide the merits of a dispute. But because “a party who has not agreed to arbitrate will

¹⁰ The default selection under an arbitration service provider's rules if no number is specified is one arbitrator unless the amount in controversy is large.

¹¹ Arbitrator service provider rules generally permit arbitrators to grant equitable relief. Nevertheless, it is common for agreements to permit a party to seek a temporary restraining order or other emergency equitable relief in a court, since this can often be accomplished more quickly than in an arbitration—particularly in the early stages of an arbitration when the arbitrator has not been selected.

¹² *Coinbase, Inc. v. Suskei*, 602 U.S. 143, 148-49 (2024). *Coinbase* also recognized a fourth layer of arbitration dispute: “What happens if parties have multiple agreements that conflict as to the third-order question of who decides arbitrability?” *Id.* at 149. As with questions 2-3, this fourth question is a matter of contract interpretation. *Id.*

¹³ *First Options of Chicago, Inc. v. Kaplan*, 514 U.S. 938, 943 (1995) (citations omitted).

normally have a right to the court's decision about the merits of its dispute," "[c]ourts should not assume that the parties agreed to arbitrate arbitrability unless there is 'clear and unmistakable' evidence that they did so."¹⁴ In other words, unless the parties' agreement is clear that the arbitrator may rule on his/her own jurisdiction, the issue of whether the merits of a dispute are arbitrable (Question 2) must be decided by a court. Parties can avoid this scenario by including a provision in their arbitration clause clearly stating that the arbitrator is the sole person permitted to rule on issues of arbitrability and jurisdiction.

III. Practical Considerations with regard to Arbitrating in the United States

1. Cost

Arbitration in the U.S. can be expensive. This is because the parties generally are required to pay three types of fees, only the first of which is required in court litigation. First, the parties must pay the general expenses associated with commercial litigation—e.g., attorneys' fees, expert witness compensation, deposition costs, etc. Second, the parties must pay the fees of the arbitration service provider (e.g., the American Arbitration Association). The amount of these fees generally depends on the amount in controversy. Bigger cases require higher administrative fees. Third, the parties must pay the compensation of the arbitrator(s), which is generally set on an hourly basis. Arbitrator rates vary significantly, with some arbitrators charging only \$300/hour and others charging in excess of \$700/hour. Once the arbitrator is required to start ruling on discovery disputes and motions, these fees begin to add up. If the case proceeds to trial (typically referred to in arbitration as the "hearing"), fees increase significantly, since the arbitrator must prepare for the trial, attend it, and then typically issue a reasoned award with factual findings.

In contrast, parties litigating in U.S. courts do not pay the judge's salary, which can be a significant cost savings in comparison to arbitration. This is not to say that the higher cost of arbitration means that parties should prefer court litigation. On the contrary, maintaining confidentiality of a dispute and having a dispute heard by an arbitrator with significant experience with a particular type of commercial transaction will often outweigh any concerns about cost.

Another way to minimize cost is by drafting restrictions on the number of arbitrators and the extent of discovery into the arbitration clause. Generally, these restrictions will be enforced. In determining whether to limit the extent of discovery, it is important to remember that proving one's case without the benefit of depositions or extensive document production can often prove difficult.

¹⁴ *Id.* at 942, 944 (quoting *AT&T Technologies, Inc. v. Communications Workers*, 475 U.S. 643, 649 (1986)).

2. Arbitrators versus Juries

In considering whether to agree to arbitration, a key factor should be whether a party prefers a jury trial. For sophisticated commercial transactions, the answer is often no.

Although the number of cases in the U.S. that proceed to jury trial has declined due to factors such as cost, unpredictability, and the growth in popularity of arbitration, jury trials remain an omnipresent facet of American litigation. Jurors are drawn from the general population in a given county and often have little experience with the subject matter of the case. Typically, jury trial results are considered less predictable than arbitration trial results.

U.S. arbitrators are almost always attorneys with significant litigation experience. Commercial dispute arbitrators are generally well-familiar with rules of procedure and evidence in the U.S., as well as the substantive law regarding contracts and business disputes.

To the extent a party wishes to obtain an arbitrator with experience in a particular area of law (e.g., transnational business disputes, employment disputes, construction disputes), that preference can be specified in the arbitration clause—particularly if the arbitration service provider (e.g., AAA) has a subject matter section dedicated to that type of dispute.

A broadly-drafted arbitration clause covering virtually all disputes is probably sufficient to defeat an opponent's demand for a jury trial. But to be safe, the agreement containing the arbitration provision should also contain a waiver-of-jury-trial clause. To be enforceable, many states require that a waiver-of-jury-trial clause be printed in conspicuous type—e.g., bold, capitalized, underlined text making the clause stand out in relation to the rest of the agreement's text.

If a contracting party wants to avoid a jury trial but the cost of litigating a dispute is a significant concern, the better option may be a bench trial. In other words, the party can drop the arbitration clause and keep the waiver-of-jury-trial clause—particularly if the party can contract for venue in a court with judges that have significant commercial dispute experience, like the Texas Business Courts.

3. Confidentiality

A party with serious reservations about the facts of a dispute becoming public record should strongly consider arbitration. In comparison to the court system, confidentiality is arguably the greatest benefit to arbitration in the U.S.

As a general rule, court filings in the U.S. are public record. It is possible to request that a court permit a particular document containing confidential, proprietary, or other sensitive information to be filed under seal so that its access by third parties is

prohibited or limited. The sealing process can be burdensome and is not always successful. Courts will generally permit the filing of documents under seal if the opposing party agrees or if the parties have executed a Confidentiality and Protective Order permitting filings to be sealed. But given the emphasis on open courts in the U.S., not all judges permit litigants to file any document they like under seal.¹⁵ Even if a court liberally permits the filing of documents under seal, the lawsuit pleadings themselves, and virtually every motion or brief, will be publicly available.

Arbitration filings are confidential and not open to the public according to the rules of the major arbitration service providers. Typically, only the proceeding to confirm an arbitration award in a court will be public record. Third parties cannot contact the arbitration service provider and obtain filings in the arbitration. Parties concerned about confidentiality can also enter into a Confidentiality and Protective Order in the arbitration that prohibits disclosure of any filings, discovery materials, or other information used in the arbitration to third parties. In short, arbitration has significant advantages for parties wishing to minimize any public record of their disputes.

4. Third-Party Discovery

Litigants generally take for granted the ability to serve subpoenas for document production and depositions on third parties in connection with a proceeding pending in the U.S.. This is not to say that serving a subpoena in a different state is always easy. The rules of civil procedure for the state in which the proceeding is pending must be complied with, as well as any applicable rules in the state where the witness is located. Rule 45 of the Federal Rules of Civil Procedure provides a fairly simple process: a subpoena can be served anywhere in the U.S., but a witness can generally only be required to produce documents or appear for a deposition within 100 miles of where the person resides, is employed, or regularly transacts business in person.¹⁶ A majority of U.S. states are party to the Uniform Interstate Depositions and Discovery Act ('UIDDA'), which provides a framework intended to make interstate discovery more efficient. States that are not a party to the UIDDA have their own procedures applicable to third-party subpoenas issued in out-of-state proceedings. Regardless of the applicable procedure, the general rule in the U.S. is that pre-trial discovery and depositions of third-parties for reasonable purposes are permitted.

That is not necessarily true with respect to pre-trial subpoenas issued to third parties in arbitration. The FAA allows arbitrators to issue subpoenas to summon "in writing any person to attend before them or any of them as a witness and in a proper case to

¹⁵ Section 108 of the U.S. Bankruptcy Code, 11 U.S.C. §§ 101 *et seq.*, requires that documents filed in a bankruptcy case remain open to the public unless certain enumerated exceptions apply (e.g., the document contains trade secrets or proprietary research or confidential information).

¹⁶ Fed. R. Civ. P. 45(a), (c). As a practice, it is common for parties to agree that documents that can be produced and shared electronically can be sent to the party issuing the subpoena from anywhere in the country.

bring with him or them any book, record, document, or paper which may be deemed material as evidence in the case.”¹⁷ Currently, there is a split among federal circuit courts regarding whether Section 7 of the FAA authorizes arbitrators to order document production from non-parties prior to an arbitration hearing.

The Second, Third, and Ninth Circuits have all determined that arbitrators cannot compel pre-hearing document discovery from non-parties.¹⁸ These Circuits’ opinions stand for the proposition that the plain language of Section 7 only authorizes arbitrators to compel non-parties to produce documents at an arbitration hearing. Stated another way, these Circuits subscribe to the rule that “[d]ocuments are only discoverable in arbitration when brought before arbitrators by a testifying witness.”¹⁹ The Fourth Circuit largely follows the rule above, except it carves out an exception where there is “special need.”²⁰ On the other hand, the Eighth Circuit has held that Section 7 grants arbitrators the implicit power “to order the production of relevant documents for review by a party prior to the hearing.”²¹ Unlike the other circuit courts, the Eighth Circuit believes such a rule furthers the efficiency of the arbitration process.²²

As a practical matter, arbitrators often do issue subpoenas to third parties for document production and depositions, regardless of whether they are enforceable if challenged. Some third parties comply with these subpoenas, while other third parties challenge them. The important thing to remember is that third-party discovery is not always as easily accomplished in arbitration as it often is in U.S. court proceedings.

5. Challenging Arbitration Awards

Challenging arbitration awards in the U.S is difficult and challenges have a low success rate. Frequently, the challenger does not necessarily expect to prevail, but is rather hoping that the award can be settled at a lower amount.

¹⁷ This section of the FAA also allows parties to petition the United States District Court where a majority of the arbitrators are sitting to compel to a third party to appear before the arbitrators according to the subpoena. 9 U.S.C. § 7.

¹⁸ *Life Receivables Trust v. Syndicate 102 at Lloyd's of London*, 549 F.3d 210, 212 (2d Cir. 2008); *Hay Grp., Inc. v. E.B.S. Acquisition Corp.*, 360 F.3d 404, 407 (3d Cir. 2004); *CVS Health Corp. v. Vividus, LLC*, 878 F.3d 703, 708 (9th Cir. 2017).

¹⁹ *Life Receivables*, 549 F.3d at 216. Courts have applied this rule to pre-hearing depositions as well. See *Stolt-Nielsen Transp. Grp., Inc. v. Celanese AG*, 430 F.3d 567, 577 (2d Cir. 2005). Under this rule, the person subpoenaed for testimony must provide the testimony at an arbitration hearing before the arbitration panel. *Id.*

²⁰ *COMSAT Corp. v. NSF*, 190 F.3d 269, 276 (4th Cir. 1999). Under this exception, a party may “petition a district court to compel pre-arbitration discovery upon a showing of special need or hardship.” *Id.* The *COMSAT* court did not define “special need.” *Id.* But found that “at a minimum, a party must demonstrate that the information it seeks is otherwise unavailable.” *Id.*

²¹ *Sec. Life Ins. Co. of Am. v. Duncanson & Holt (in Re Sec. Life Ins. Co. of Am.)*, 228 F.3d 865, 871 (8th Cir. 2000).

²² *Id.*

Once the arbitrator issues an award, the prevailing party must confirm the award in a court of appropriate jurisdiction to obtain an enforceable judgment that can be used to seize assets. If the FAA governs the arbitration, then the application to confirm the award must be made within one year of the award being issued.²³ The application to confirm the arbitration award can be challenged by the losing party, but the grounds for doing so are generally very limited. The exclusive grounds for vacating an award under the FAA are set forth in Section 10.²⁴ These grounds address situations where the award was procured by fraud or arbitrator corruption, arbitrator misconduct, or an arbitrator exceeding their powers—in short, drastic situations not present in the vast majority of arbitrations. An award can also be modified or corrected under Section 11 for issues such as material miscalculations, material mistakes in describing a person, thing, or property, or where arbitrators have awarded upon a matter not submitted to them.²⁵ Some state statutes contain alternative grounds for vacating or modifying an award. Some states also permit parties to contract for additional grounds to vacate or modify an award that are not listed in a statute.²⁶

If a party challenges the confirmation of an award in court and loses (as is usually the case), the losing party generally has a right to appeal the confirmation decision. Such an appeal is rarely successful, given the very limited grounds for challenging confirmation.²⁷ Notably, the right to appeal an order confirming an award under the FAA may be waived in the arbitration clause, while the right to seek vacatur of an award at the district court level may not.²⁸

6. Enforcement Abroad

Generally speaking, it is significantly easier to enforce a U.S. arbitration award in a foreign country than it is to enforce a civil judgment entered by a court. This is because the U.S. is a party to conventions intended to streamline the process for enforcing arbitration awards, most significantly the United States Convention on the Recognition and Enforcement of Foreign Arbitral Awards (commonly referred to as the New York Convention). As of 2025, there are 172 contracting states to the New York Convention, making enforcement of United States arbitration awards relatively simple in comparison to enforcement of civil judgments.

²³ 9 U.S.C. § 9.

²⁴ For a complete list of grounds to vacate an arbitration award under the FAA, see § 10; *see also Hall St. Assocs., L.L.C. v. Mattel, Inc.*, 552 U.S. 576, 588 (2008) (holding that the grounds for vacating, modifying, or correcting an award under the FAA are the sole means of doing so).

²⁵ For a complete list of grounds to modify or correct an arbitration award under the FAA, see § 11.

²⁶ *Forest Oil Corp. v. El Rucio Land & Cattle Co.*, 518 S.W.3d 422, 432 (Tex. 2017) (discussing expanded grounds for review under the Texas Arbitration Act).

²⁷ 9 U.S.C. § 16 lists other appeals that may be taken under the FAA other than an appeal from an order confirming or denying confirmation of an award. For example, an order refusing to stay litigation so that arbitration can proceed is appealable.

²⁸ *Vantage Deepwater Co. v. Petrobras Am., Inc.*, 966 F.3d 361, 368-69 (5th Cir. 2020) (discussing cases addressing waivers of appeal of arbitration awards).

Conversely, the U.S. is not a party to any similar treaty governing the enforcement of U.S. judgment abroad. The U.S. has signed but not ratified the Convention of 2 July 2019 on the Recognition and Enforcement of Foreign Judgments in Civil or Commercial Matters, commonly known as the Hague Judgments Convention. Accordingly, the Hague Judgments Convention cannot currently be used to enforce U.S. judgments abroad.

A comparison of how to enforce a U.S. arbitration award versus a U.S. civil judgment abroad is beyond the scope of this article. Suffice to say that arbitration remains the preferable dispute resolution process for a party wishing to streamline enforcement of the award outside of the U.S.

IV. Conclusion

Whether to agree to arbitration is one of the most important considerations parties should take into account when drafting dispute resolution provisions into their agreements. Arbitration in the U.S. has significant benefits, such as confidentiality and adjudication of disputes by individuals with specialized experience. It can also be costly and the ability to conduct third-party discovery may be limited. Parties should consider the issues outlined in this article when deciding whether to agree to arbitration and when drafting the arbitration clause. Consulting a qualified U.S.-based attorney is always advisable.

ICC FraudNet
Global Annual Report 2025

Recent Developments in U.S. Foreign Sovereign Immunity Jurisprudence

TARA PLOCHOCKI



Recent Developments in U.S. Foreign Sovereign Immunity Jurisprudence

Tara Plochocki
Sequor Law

As litigation involving sovereigns proliferates, U.S. courts have had increased opportunities to refine the contours of foreign sovereign immunity. This past year alone, the U.S. Supreme Court issued two opinions refining the contours of the Foreign Sovereign Immunities Act (“FSIA”) while lower courts evolved the jurisprudence on compensable losses and attachable assets. This article surveys some of the most significant cases to transpire within the last year and offers guidance on how award and judgment creditors might shape their litigation strategies in light of these developments.

Overview of U.S. Law on Foreign Sovereign Immunity

All cases against foreign sovereigns in the United States must establish that the court has subject matter jurisdiction over the case. That is, the petitioner/plaintiff must show that the federal court has been given the power to hear the specific case. In the case of foreign sovereigns, subject matter jurisdiction exists if there is an absence of immunity. Foreign sovereigns and their instrumentalities are immune unless one of six exceptions applies: (1) waiver, (2) commercial activity, (3) expropriations, (4) rights in property taken in violation of international law that has a commercial nexus with the United States, (5) noncommercial torts, and (6) enforcement of arbitral agreements. There is also an exception to claims against state sponsors of terror, which has been interpreted to apply only to a handful of states.

Likewise, foreign sovereigns’ property is immune from attachment by default, and attachable if such property is in the United States, used in commercial activity, and the

execution relates to a judgment arising out or relating to an action for which there is no immunity. These largely track the exceptions to immunity listed above, for example, judgments confirming arbitral awards, relating to claims arising out of commercial activity in the U.S., relating to a taking in violation of international law, and more.

1. *Republic of Hungary v. Simon* Imposes Tracing Requirements on Property in Expropriation Claims

The most significant sovereign immunity case this term was *Republic of Hungary v. Simon*, 145 S. Ct. 480 (2025), which resulted in a ruling narrowing the scope of the expropriation exception. This exception states that foreign sovereigns are not immune from jurisdiction in any case:

in which rights in property taken in violation of international law are in issue and that property or any property exchanged for such property is present in the United States in connection with a commercial activity carried on in the United States by the foreign state; or that property or any property exchanged for such property is owned or operated by an agency or instrumentality of the foreign state and that agency or instrumentality is engaged in a commercial activity in the United States.

28 U.S.C. § 1605(a)(3). The exception means that when the defendant is the foreign state, the expropriated property must be in the United States. When the defendant is an instrumentality, then the property need not be in the United States, but it—or property exchanged for it—must be owned by the instrumentality doing business in the United States. Whether the foreign sovereign itself loses immunity if it gives the property to an agency or instrumentality is a question that has been posed to the Supreme Court for resolution next term.¹

The United States is the only country to have codified an unlawful expropriation exception—generally an uncompensated taking is understood to be a *sovereign* act, not a commercial one. In recent years, U.S. courts have issued rulings that narrow its application. For instance, the Supreme Court ruled that the exception applied only to property taken from foreigners by a foreign sovereign because a government cannot expropriate property from its own citizens under *international* law² and that the alleged facts must show a legally valid claim that a taking occurred, as opposed to just a plausible claim that one occurred.³ And, the exception only applies to takings during peacetime; this past year, a D.C. federal court dismissed a different claim against Hungary by Italian Holocaust survivors because the artwork at issue was seized during wartime.⁴ As such, it was public act of a sovereign subject to the international laws of

¹ Petition for a Writ of Certiorari, *Agudas Chasidei Chabad of United States v. Russian Federation* (2025) (No. 24-909).

² *Fed. Rep. of Germany v. Philipp*, 592 U.S. 169 (2021).

³ *Bolivarian Rep. of Venez. v. Helmerich & Payne Int'l Drilling Co.*, 581 U.S. 170, 187 (2017).

⁴ *de Csepel v. Rep. of Hungary*, 752 F. Supp. 3d 147, 162 (D.D.C. 2024)

war and entitled to immunity as opposed to a private act interfering with property rights.

In *Republic of Hungary v. Simon*, the Court further circumscribed the scope of the exception. In this case, Jewish survivors of the Hungarian Holocaust and their heirs sued Hungary and its national railway, MAV, seeking damages for property expropriated during World War II. These plaintiffs alleged that Hungary and the MAV liquidated the expropriated property and commingled the proceeds with other state treasury funds. While the plaintiffs could not trace their funds from their or their heirs' specific property to the United States, they alleged that funds from the commingled accounts were "exchanged for" the expropriated property later used in commercial activities in the United States by Hungary and that its railway still had some of the commingled funds. Hungary allegedly used funds from its treasury to issue bonds in the United States and to purchase military equipment in the U.S.; MAV also engages in commercial activity in the United States, including by maintaining an agency that sells tickets, books reservations, and conducts similar business. Under this theory, the plaintiffs claimed that they satisfied the commercial nexus requirement of the expropriation exception to sovereign immunity.

Hungary and MAV argued that the commingling theory was not enough; that plaintiffs must trace their property or property "exchanged for" their property to the United States, despite the passage of time and the horrible circumstances of the taking. The difficulty of doing so is obvious. Countries that take property in violation of international law do not publish registers of what they have done with it, and this was certainly not the case for Hungary as it carried out a genocide in the 1940s. And in cases of liquidated expropriated property, it is not clear how a plaintiff is supposed to identify the specific funds exchanged for the stolen property and trace them to the United States, since once deposited, those funds are indistinguishable from the rest of the money in the account.

In this way, the plaintiffs presented a compelling argument for construing the expropriation exception equitably; rejecting the commingling theory and imposing a tracing obligation would effectively terminate the expropriation exception altogether. The Supreme Court disagreed and unanimously ruled that allegations of the use of funds in commercial activity in the United States from an account holding the commingled proceeds of expropriated property does not give rise to a plausible inference that funds exchanged for the expropriated property are in the United States.

The Supreme Court offered examples of commingling that might suffice to anchor a claim in the U.S., such as identifying a U.S. bank account in which the proceeds of the sale of expropriated property were deposited with other funds. But this is an incredibly unlikely scenario.

The Court's decision rightly recognizes that FSIA was intended to provide blanket foreign sovereign immunity with specific, limited exceptions. That U.S. law allows

expropriation cases to proceed at all makes it an outlier; the Court’s ruling reflects that Congress would not have intended there to be such a low bar to filing suit. But the Court’s decision runs directly contrary to a robust body of case law in which courts have held that because money is fungible, it is not possible to determine which commingled funds belong to whom. In forfeiture cases, once funds obtained from illegal activity are combined with funds from a lawful activity, courts overwhelmingly treat the clean and tainted funds as indistinguishable, impose no tracing requirement at all before permitting the government to seize a portion of them. Instead deeming some portion of the account to be “criminally-derived property” if proceeds of illicit activity were in the account at any point. In so ruling, courts have observed that requiring the government to trace each dollar seized to some criminal activity would allow the simple act of commingling to effectively defeat prosecution for money laundering. Because of the ruling in *Republic of Hungary v. Simon* foreign governments may likewise preempt expropriation lawsuits in the United States by commingling the proceeds from the sale of expropriated property in their general treasury.

As a result of *Republic of Hungary v. Simon*, human rights claimants may no longer be able to use the expropriation exception to foreign sovereign immunity to recover their historic losses because the pleading burden is too difficult. Litigants pursuing claims under the expropriation exception to the FSIA often struggle to make the showing that the expropriated property or what was exchanged for it is in the United States. Conversely, it is unlikely that *Republic of Hungary v. Simon* will have a significant impact on investors or corporations involved in foreign investment susceptible to unlawful expropriation. Those investments are generally subject to agreements or treaties with arbitration provisions, and they can obtain recognition of their arbitral awards under a different exception to the FSIA.

2. *CC/Devas (Mauritius) Ltd. v. Antrix Corp.* Confirms that the FSIA does not require minimum contacts for jurisdiction.

In *CC/Devas (Mauritius) Ltd. v. Antrix Corp.*, 145 S. Ct. 1572 (2025), the Supreme Court clarified an issue that no one really questioned, not even the appellate court that issued the underlying decision. In an action arising out of recognition of a foreign arbitral award issued in favor of Devas Multimedia Private Ltd. against Antrix Corporation Ltd., wholly owned and operated by the Republic of India, the U.S. Court of Appeals for the Ninth Circuit decided that under the FSIA, a petitioner/plaintiff must demonstrate the that foreign state—here, India’s instrumentality Antrix—has “minimum contacts” with the United States.

The minimum contacts test was articulated in *International Shoe Co. v. Washington*,⁵ and was deemed necessary to satisfy the due process requirements of the Fourteenth Amendment to the U.S. Constitution, which applies to the individual U.S. states. The test inquires whether the defendant has sufficient ties to the State in which the suit is

⁵ 326 U.S. 310, 311 (1945).

filed such that it is fair to exercise power over it. For foreign defendants—whether from another U.S. State or a foreign country—the test looks for contacts between the underlying claim and the selected jurisdiction.

In *CC/Devas*, the Ninth Circuit reluctantly relied on decades-old circuit precedent by which it felt bound. The Supreme Court took the opportunity to resolve this outlier position; it held, unanimously, that the FSIA contains no implied minimum contacts test. To the extent that the FSIA requires a nexus with the U.S. to satisfy an exception to sovereign immunity, the statute itself so indicates. Examples include “rights in immovable property situated in the United States,” “commercial activity carried on in the United States by the foreign state,” or “commercial activity of the foreign state elsewhere” that “causes a direct effect in the United States.”

The *CC/Devas* case is notable for what the Court did *not* decide. Antrix also argued that foreign corporations are entitled to due process under the Fifth Amendment to the U.S. Constitution. Foreign states are traditionally not entitled to due process because the Due Process Clause only applies to “persons”, which foreign states are not. The FSIA defines a “foreign state” to include foreign corporations that are instrumentalities of the foreign sovereign. But under ordinary due process analysis, a corporation, including a foreign corporation, counts as a “person” with due process rights. This means that they are entitled to challenge the court’s exercise of jurisdiction over it. Antrix thus argued that the FSIA, as a statute, cannot strip foreign corporations of their constitutional rights, which are superior to statutory laws in the United States, and so the minimum contacts test should apply.

The Supreme Court declined to address that argument, sending it back to the lower courts for resolution, but Antrix’s argument has already been rejected in part. In *Fuld v. PLO*, 606 U.S. 1 (2025), decided just two weeks after *CC/Devas*, the Supreme Court held that the Fifth Amendment does not impose the same jurisdictional limitations as the Fourteenth Amendment does against individual U.S. States, and thus the minimum contacts test does *not* constrain the federal government in the exercise of its sovereignty, which is broader than the States’. The Supreme Court conceded that the federal government’s power to hale foreign defendants into U.S. courts is not without any limits but declined to decide the outer bounds of that power. The Supreme Court will have occasion to decide whether Congress exceeded that power in the FSIA when the *CC/Devas v. Antrix* if the parties appeal from the next round of proceedings.

3. Recovering and Attaching Intangible Interests Under the FSIA

Finally, three recent cases highlight that the FSIA provides recourse to recover and attach intangible property interests.

In the long-running case concerning losses arising out of Argentina’s seizure of shares of YPF, a petroleum company, the U.S. District Court for the Southern District of

New York ordered Argentina to turnover its 51% shareholding in YPF.⁶ YPF is listed as the holder of the same class of shares for purchase on the New York Stock Exchange, inarguably placing them within the commercial activity exception to sovereign immunity. The court ruled that the expropriated shares were attachable under New York turnover law as “uncertificated securities.” The court thus ordered Argentina to bring the shares from where they were held in Argentina into a global custody account at the Bank of New York Mellon in New York, after which they would qualify as property within the United States subject to execution under the FSIA. Although this is only partial satisfaction of the outstanding \$16.1 billion judgment against Argentina, the court-ordered transfer of this interest materially improves the position of Argentina’s creditors. That order has been stayed pending appeal.

The YPF turnover is the second of Argentina’s major courtroom losses this past year. It earlier challenged the decision by the U.S. Court of Appeals for the Second Circuit, in which the court affirmed a ruling that creditors could attach Argentina’s reversionary interests in collateralized bonds that had been offered as part of a sovereign debt relief program.⁷ The collateralized bonds were backed by U.S. Treasury bonds and Deutsche Mark bonds and due in 2023, at which point, the Federal Reserve Bank of New York liquidated the collateral to pay bondholders. Argentina had interests in the remainder.

Judgment creditors—holders of previous defaulted bonds issued by Argentina—sought to attach the intangible reversionary interests to satisfy their judgment. Argentina argued that these interests were immune from attachment because they were owned by the central bank of Argentina and not in the United States because the Deutsche Mark bonds were in Germany. The court disagreed on both counts. Not only had the interests been used in commercial activity in the U.S. as an incentive for bondholders to transact, but the key determination is where the reversionary interests lie, not the collateral itself. Because the collateral agent in New York was the entity charged with honoring Argentina’s reversionary interests, the Second Circuit confirmed that the location of the property interest was in the United States.

Actions based on intangible property likewise serve as a basis to bring a claim against a foreign sovereign, even if the foreign sovereign never seizes the intangible property for itself. A D.C. federal court recently held that the U.S.-based parent shareholder of a Venezuelan subsidiary had a valid expropriation claim based on the takeover of that subsidiary’s assets and operations by Venezuela state-owned oil company PDVSA.⁸ The U.S. parent shareholder based its claim on the expropriation of its U.S.-based shareholder rights in the subsidiary. While PDVSA did not technically take the U.S. parent shareholder’s shares or formally divest it of ownership of those shares, it did render them valueless by nationalizing the subsidiary in violation of international law.

⁶ *Petersen Energia Inversora, S.A.U. v. Argentine Rep.*, No. 15-cv-02739, 2025 U.S. Dist. LEXIS 123643 (S.D.N.Y. June 30, 2025).

⁷ *Attestor Master Value Fund LP v. Argentina*, 113 F.4th 220, 228 (2d Cir. 2024), *cert. denied sub nom. Argentina v. Attestor Master Value*, 145 S. Ct. 1141 (2025).

⁸ *Helmerich v. Petroleos de Venezuela, S.A.*, 754 F. Supp. 3d 29, 40 (D.D.C. 2024).

By proving that all the assets of the subsidiary had been taken and no commercial operations did or could continue, the court recognized a valid expropriation claim under FSIA.

Looking forward, we can expect that U.S. courts will continue to further refine the nuances of immunity for foreign states and their property and that they will have ample occasion to do so. With Syria's designation as a state sponsor of terror under review, it is unclear what will happen to cases filed under that exception to the FSIA if such designation is removed. And the U.S. courts are bound to find themselves in further conflict with foreign laws which states believe should apply in the United States. For instance, Spain has sought review from the Supreme Court of a decision to recognize arbitral awards that are unenforceable per recent CJEU decisions.⁹ Courts both in the United States and abroad will need to ensure that their rulings maintain consistent fidelity to law in spite of inconstant geopolitical stability.

⁹ Petition for a Writ of Certiorari, *Kingdom of Spain v. Blasket Renewable Investments LLC* (2025) (No. 24-1130).

ICC FraudNet
Global Annual Report 2025

Asset Investigations in High Net Worth Divorces

DC PAGE



Asset Investigations in High Net Worth Divorces

**DC Page
V2 Global**

Divorces can be messy, especially when substantial assets are involved, making them more contentious. When higher stakes are at play, a spouse might try to hide income or assets. In such cases, an experienced investigator can often help uncover the truth and identify all assets.

There are many ways a spouse might try to hide assets or income, including purchasing and transferring assets (such as real estate) to a family member, friend, or lover; maintaining undisclosed bank accounts; using cryptocurrency accounts; not reporting or underreporting income or dividends from business ventures or investments; claiming non-existent debts (“sham loans”); buying high-value luxury items such as jewelry, art, vehicles, yachts, or private jets; using shell and offshore companies to buy assets; purchasing gold, silver, or diamonds and hiding them offshore or under someone else’s name; parking cash in offshore bank accounts in jurisdictions with strict privacy laws; and sending wire transfers disguised as payments.

A real-life example of a spouse hiding assets involved a husband concealing the existence of an entity he controlled, which he used to stash large amounts of cash in a company-controlled account. An investigation into his personal and living expenses led investigators to the company, giving his wife’s counsel legal justification for the relevant discovery requests. Another example involved a spouse making sizable vendor payments from his consulting firm to fake offshore vendors that he owned and controlled. A thorough investigation eventually uncovered the true identities of the vendors and the spouse’s fraudulent intent.

An investigator analyzing a spouse suspected of hiding assets should begin by developing a detailed profile of the individual, collecting as much information as possible. It is essential to spend time creating an accurate and comprehensive profile to understand the person and the person's methods and motives. The profile should include details about the individual and the individual's family, close friends, and romantic partners, including phone numbers, physical addresses, email addresses, social media accounts, businesses, ventures, investments, credit information, border crossings and customs declarations, vehicle information, and utilities' data. When building a profile, an investigator must not overlook the subject's lifestyle and psychological aspects, such as character, personality, habits, hobbies, fetishes, vices, predispositions, vulnerabilities, and any known psychological issues, like drug abuse.

An example demonstrating the importance of a well-developed profile involved a case where a thorough examination and analysis of the subject's profile revealed the identity of a girlfriend living in an offshore jurisdiction. Further inquiries showed that funds had been diverted over many years to her and the companies she controlled. These companies owned real estate, cars, boats, and numerous bank accounts.

Once a profile is created, an investigator will utilize various investigative techniques and tools to identify and locate hidden assets. These include databases, digital and computer forensics, public records, corporate records, banking records, artificial intelligence, confidential sources, interviews with associates, friends, and enemies, pretext approaches, quasi and fully covert activities, and surveillance. When legally permitted in the jurisdiction, examining the subject's garbage can prove to be a valuable source of relevant information.

While surveillance is the most common tool used in divorce cases, it is mainly employed to catch a cheating spouse since infidelity often has no effect on divorce proceedings in many states across the United States. On the other hand, covert activities, pretext approaches, or garbology—when conducted within the legal limits of the relevant jurisdiction—often yield better legal results by uncovering hidden assets and impacting the divorce settlement.

It should be noted that in many jurisdictions, garbage can not only provide us with information and intelligence, but it can also be admitted as evidence when properly handled. For example, in one case, garbage retrieved from an estranged spouse's residence revealed bank statements from undisclosed accounts and insurance payment receipts for expensive artwork that had also not been disclosed during the discovery process. Counsel was able to introduce the receipts as evidence to obtain a favorable outcome for the other spouse.

In conclusion, experienced investigators in high-net-worth divorce cases provide many benefits and efficiencies. Not only can skilled investigators uncover hidden assets, but the evidence and intelligence they gather can also strengthen the attorney's case and improve negotiating power during settlement discussions.

Strategic Partners



BDO is an international network of public accounting, tax and advisory firms which perform professional services under the name of BDO.



FRA is a leading global forensic accounting and eDiscovery consultancy, that works with clients to identify, analyse, and mitigate risks related to financial misconduct. With expertise in forensic accounting, data governance, and compliance, FRA is a trusted partner in the fight against fraud, bribery, and corruption.



Highgate is a global market leader in dispute resolution. They shape the environment outside the courtroom to help win disputes. Working with legal advisers and investigators, Highgate deploys creative and intelligence-driven strategies to bring the other side to the negotiating table.



Grant Thornton is one of the world's largest professional services networks of independent accounting and consulting member firms that provide assurance, tax and advisory services to privately held businesses, public interest entities, and public sector entities.



GreyList Trace Limited is a UK based fintech company that has developed artificial intelligence risk screening technology. Its cutting-edge proprietary algorithm software can legally and non-invasively identify any one or two-way connections between any pair of email addresses.



Mintz Group is a corporate investigations firm that gathers information before hiring, before transactions, during litigation disputes and after frauds, all over the world.



V2 Global provides risk mitigation and strategic solutions on a global scale. Focusing on the acquisition and synthesis of information, they specialise in crisis and risk management, investigatory and strategic advisory services in areas of business intelligence, cyber and data security and forensics.



4 New Square are a leading set of barristers' chambers and have a stellar reputation in a wide range of fields, including commercial dispute resolution and chancery commercial litigation, offshore disputes, international arbitration, civil fraud, financial claims and costs. They regularly appear at all levels in courts and arbitrations worldwide.

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

www.iccfraudnet.org

Follow us

