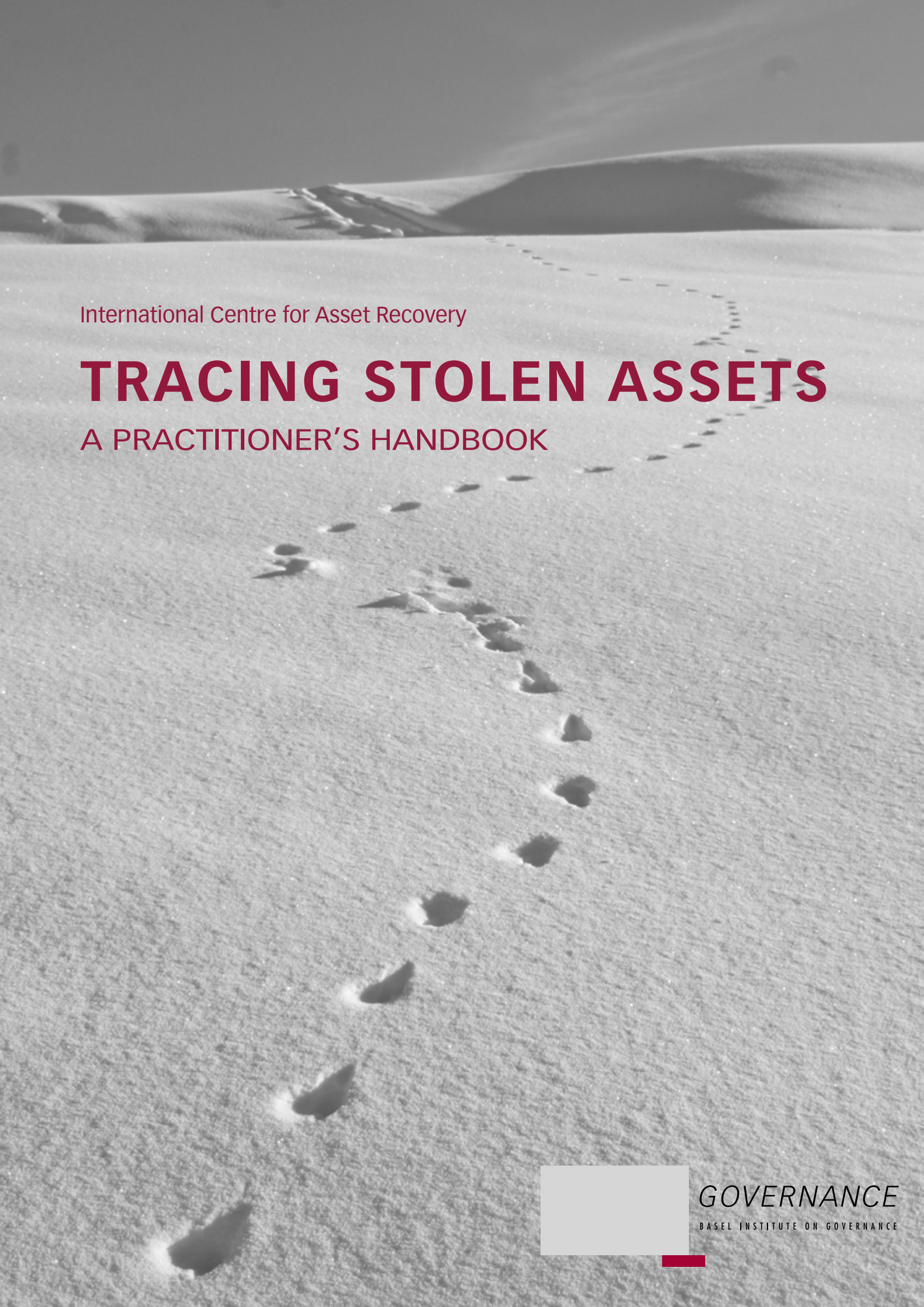


International Centre for Asset Recovery

TRACING STOLEN ASSETS

A PRACTITIONER'S HANDBOOK

GOVERNANCE
BASEL INSTITUTE ON GOVERNANCE

Steinenring 60, 4051 Basel, Switzerland
Phone +41 61 205 55 11, Fax +41 61 205 55 19
www.baselgovernance.org, info@baselgovernance.org

Cover design by Peter Huppertz, Basel Institute on Governance

Tracing Stolen Assets:
A Practitioner's Handbook

Table of Contents

Preface

Asset Recovery is a promising strategy against graft, embezzlement of public funds and corruption. The United Nations Convention against Corruption (UNCAC) and, in particular, the joint initiative by the World Bank and the United Nations Office on Drugs and Crime (UNODC) termed StAR (Stolen Assets Recovery Initiative), have pushed the issue up the political agenda. Much is being done currently in financial centres to allow for more effective freezing, confiscation, mutual legal assistance and repatriation of assets.

However, effective asset recovery starts much earlier. In most cases, the decisive steps determining success or failure are taken in the very first moments of asset tracing:

Ample experience with money laundering tells how easy it is to obscure the traces of looted assets. We have become used to 'gatekeepers', frequently profiting from professional confidentiality (e.g., lawyers) setting up structures, based on shell corporations, often registered in offshore locations, where the company register is either not public or contains little relevant information about the actual beneficial owners. Such 'IBCs' (International Business Cooperations) would then be used to open bank accounts at locations where customer due diligence is not up to world standard, and where the likelihood of mutual legal assistance is slim. These structures can create a dense smoke screen.

Piercing the veil is a formidable task. It involves the cooperation of 'gatekeepers' (banks, financial intermediaries or lawyers), Financial Intelligence Units (FIUs) and law enforcement agencies as well as public and private forensics specialists. They have to follow up leads, use various forms of intelligence and cooperate internationally. Technology also has an important role to play in facilitating such cooperation, employing systematic and proven techniques during an investigation and constructing the money trail in cases involving stolen assets.

Obviously, once ill-gotten gains have been traced to a specific location, the legal action sets in: restraint or freezing orders are of paramount importance. It is fundamental to ensure that funds can be blocked on a provisional basis in just a few hours after detection. Any jurisdiction missing this target has to be considered a safe haven for those committing graft. Obviously, the seizure thereafter is a matter for due process in the course of the further proceedings. It is crucial, however, that the funds stay frozen while the deliberations continue.

At a time, when knowledge about mutual legal assistance and various options of criminal conviction and non-conviction based confiscation are growing, this handbook intends to direct the spotlight on a very practical but essential precondition for asset recovery: asset tracing.

Prof Dr Mark Pieth
President of the Board
Basel Institute on Governance

Contributors

PHYLLIS ATKINSON has been an Advocate of the High Court in South Africa since 1981, and spent twenty-three years as a Public Prosecutor, five years of which were served as an Advocate in the Office of the Director of Public Prosecutions and twelve years with the Office for Serious Economic Offences. This office later merged with the Directorate of Special Operations – also known as the Scorpions – where Phyllis was a Deputy Director of Public Prosecutions at the time of her resignation in June 2004. Prior to joining the International Centre for Asset Recovery (ICAR) at the Basel Institute on Governance on 1 June 2009, she was a Principal at Deloitte Forensic & Dispute Services in South Africa where she played a national role in the Forensic team, driving growth in cross-border services, including Anti-Money Laundering and Anti-Corruption training initiatives, amongst others. A Certified Fraud Examiner, Phyllis has been involved in numerous high profile commercial crime investigations and prosecutions over the years, and compiled numerous requests for mutual legal assistance in the process. She has been actively involved in training for many years, and currently works as a Senior Asset Recovery Specialist for ICAR, participating in training interventions to help developing countries recover stolen assets.

ALAN BACARESE is a United Kingdom Senior Crown Prosecutor. He spent 14 years prosecuting criminal activity ranging from fraud to murder before transferring to Crown Prosecution Services (CPS) headquarters in London in 2001 to undertake criminal justice policy work and specialised work on human rights. In May 2007, he was seconded by the CPS to the Basel Institute on Governance's newly-created International Centre for Asset Recovery (ICAR), based in Basel, Switzerland, where he continues to provide legal and practical expertise in the growing field of international asset recovery.

STEPHEN BAKER is an English barrister and Jersey advocate. He is a partner of BakerPlatt, a law firm based in Jersey, Channel Islands, specialising in litigation, financial crime and regulatory matters. Stephen has regularly acted for foreign governments in asset recovery actions and is frequently instructed by Jersey's Attorney General in complex fraud and money laundering cases, particularly those with an international and political dimension.

YARA ESQUIVEL was a Public Prosecutor at the Costa Rican Office of Economic and Corruption related Crimes from 2000-2006, where she was in charge of the investigation and trial of grand corruption cases involving 2 former heads of State. In 2006, she took a position as a regional investigator in the Office of Internal Oversight Services of the United Nations in Kenya, where she was posted for one year to investigate fraud, corruption and malfeasance within the various Peace Keeping Missions operating in Africa. She joined the International Centre for Asset Recovery (ICAR) in 2007 as an anti-corruption specialist, where she worked with various law enforcement agencies from developing countries in strengthening their capacity to investigate corruption, fraud and money laundering to ultimately recover proceeds of crime. She has delivered training courses and presentations in several international events. Currently, she is posted at the World Bank as an investigator for the Integrity Vice Presidency, with the mandate to investigate fraud and corruption in bank projects. Yara has a law degree from the Universidad de Costa Rica, she participated in the Postgraduate Specialist Program on Investigation and Evidence in the Criminal Process at the Universidad Castilla La Mancha in Spain and is currently writing her master's thesis on the topic of Asset Recovery for the International Human Rights Law program at Oxford University.

CHARLES GOREDEMA has been with the Cape Town office of the Institute for Security Studies since August 2000. He heads the Organised Crime and Money Laundering Programme. Over the past ten years, he has been involved in research and networking in the formulation of responses to economic crime, organised crime and money laundering. He has worked in these areas in southern Africa, as well as Kenya and Uganda. He organises meetings, workshops, seminars and conferences in the region and beyond. Charles has written many articles and reports, and contributed to books on the subjects above.
Charles is currently managing research projects on trends of organised crime and money laundering in Angola, Botswana, Kenya, Lesotho, Malawi, Mauritius, Mozambique, Namibia, South Africa, Swaziland, Tanzania, Uganda, Zambia and Zimbabwe. He holds a Bachelor of Laws degree (University of Zimbabwe) and a Master of Laws degree (University of London). Charles worked as a prosecutor for seven years, and as a lecturer in law at three universities in southern Africa for 12 years.

MARTIN KORTE is a Senior Consultant with the Ernst & Young Fraud Investigation and Dispute Service Department based in Frankfurt, Germany. He is specialised in fraud and asset tracing investigations as well as in forensic accounting related issues. Martin's industry focus also includes banking and finance.

THOMAS D. LASICH is currently the Head of Training for the Basel Institute on Governance, International Centre for Asset Recovery (ICAR) section in Switzerland. The Institute provides technical assistance to countries on political corruption and money laundering issues. Tom designs, creates and manages technical training programs that are delivered by ICAR in countries on all the major continents including Africa, Asia, South America, and Europe.
Tom, a graduate of the University of Santa Clara (California) with a degree in Finance, has worked in federal law enforcement in the United States (US) conducting financial investigations and presenting money laundering, anti-corruption and financial investigative technique training programs for 37 years. He began his career as a special agent with the Internal Revenue Service (IRS), Criminal Investigation, in 1972 and worked 20 years as a special agent and manager. In 1991 he accepted a position at the Federal Law Enforcement Training Centre (FLETC) as the Assistant Chief of the Financial Fraud Institute. Two years later he moved to Washington DC as a special agent with the Office of the Inspector General, Resolution Trust Corporation, a newly formed government agency created to investigate the failed savings and loan industry. In 1996 Tom returned to the IRS, Criminal Investigation, as a special agent in the international division. He conducted money laundering and financial investigations of organised crime members, major corporations, narcotics syndicates and political figures throughout the US, Europe and the Pacific Rim.
Following his retirement in 1998 from Federal employment, Tom became a Program Coordinator with the Federal Law Enforcement Training Centre, Computer and Financial Investigations Division. As the project manager for all High Intensity Financial Crime Areas (HIFCA) training relating to money laundering and asset forfeiture he designed and coordinated training programs throughout the United States, Botswana (Africa), Poland, Russia, Hungary, Moldova, the United Arab Emirates, Kuwait, Kosovo, Macedonia, Colombia, Puerto Rico, and the US Virgin Islands.

HARI MULUKUTLA is a business information systems professional focusing on governance, anti-corruption and stolen asset recovery, providing expertise to both the public and private sectors. Hari, based in the United States, advises developing countries on projects to introduce data-driven governance techniques and modernisation of national information technology infrastructures and has experience implementing IT solutions within law enforcement agencies, anti-corruption bodies,

and financial intelligence units. Hari has spoken at international conferences about the importance of information technology and process management within the anti-corruption and asset recovery context. Until recently, he was the head of the IT business development unit at the International Centre for Asset Recovery (ICAR), Basel Institute on Governance.

CHRISTIAN MUTH is a Senior Consultant with the Ernst & Young Fraud Investigation and Dispute Service Department based in Frankfurt, Germany. Being a former military intelligence officer, he is today specialised in all intelligence related aspects of fraud and asset tracing investigations.

KEITH OLIVER is a Senior Partner at Peters & Peters and heads the firm's specialist Commercial Litigation/Civil Fraud and Asset Tracing Team. He specialises in international and domestic civil and commercial fraud litigation, asset tracing/ recovery, regulatory, insolvency and trust litigation. Keith is recognised as one of the leading experts in civil fraud and asset tracing with extensive experience at the cutting edge of domestic and international fraud and asset tracing litigation (including the use of emergency procedures (freezing orders, search and seizure orders, passport orders). He is frequently engaged in multi-jurisdictional actions in the USA, continental Europe and worldwide.

MARK PIETH is Professor of Criminal Law and Criminology at the University of Basel, Switzerland, and co-founder and Chairman of the Board of the Basel Institute on Governance. From 1989 to 1993, he headed the section on Economic and Organised Crime in the Swiss Federal Department of Justice and Police. Since 1990, he has been Chairman of the OECD Working Group on Bribery in International Business Transactions. From 2003 to 2005, he was a Member of the Independent Inquiry Committee into the Iraq Oil-for-Food Programme by the UN Secretary General. Prof. Pieth is also a Member of the Wolfsberg Anti-Money Laundering (AML) Banking Initiative and a Board Member of the World Economic Forum's Partnering against Corruption Initiative (PACI).

MARKUS J. RÜEGG is an Analyst and IT Officer in the Financial Intelligence Unit, Principality of Liechtenstein. Since 2001, Markus has been a member of the Training and IT Working Group of the Egmont Group. Trained in operational crime analysis, forensic computing and combating cyber crime techniques, Markus had a long career in law enforcement as an investigator at cantonal level and at federal level as Head of General Crime Unit of the Swiss Federal Criminal Police, in Berne, Switzerland. Markus has implemented a number of IT projects and developed training programs internationally for developing countries in the areas of financial intelligence, operational, tactical and strategic crime analysis.

ED SHORROCK, FCA is Director of Forensic & Regulatory Services at BakerPlatt, a law firm based in Jersey, Channel Islands. Ed routinely works with regulators and court appointed officials involved in regulatory, asset freezing and insolvency matters. Ed is the author of a variety of publications on regulatory matters and lectures on the topic of financial crime at conferences and as part of professional education programs.

DANIEL THELESKLAF is a lawyer by profession. After a career in the private sector at Swiss Life and Dresdner Bank, he joined the Swiss Federal office of Police in 1998 to become the first Director of Switzerland's FIU. In 2002/2003, he led the Due Diligence Unit (the AML regulator) in Liechtenstein and, since 2000, he has been a board member of Transparency International, Switzerland. He is now engaged in various anti-money laundering, counter-terrorist financing and anti-corruption projects and technical assistance missions for the OECD, the UN, the Council of Europe, the OSCE and the IMF. In 2008, he became Co-Director of the Basel Institute on Governance.

ARNO THUERIG is a director of KPMG Forensic in Zurich, Switzerland. He is an attorney-at-law and holds a master degree in Economic Crime Investigation. He has more than ten years of hands-on experience as examining magistrate (state attorney) of the canton of Zurich with specialization in investigating all forms of economic crimes such as investment fraud, stock market manipulations, money laundering offences and in-house delinquency.

BASEL INSTITUTE ON GOVERNANCE
INTERNATIONAL CENTRE FOR ASSET RECOVERY

Empowerment for the tracing of stolen assets

The Basel Institute on Governance is an independent non-profit think tank conducting research, policy development and capacity building in the areas of corporate and public governance, anti-corruption and asset tracing and recovery. Based in Basel, Switzerland, and associated with the University of Basel, the Institute co-operates with governments and non-government organisations from around the world. Notably, the Institute also acts as facilitator in debates on delicate corporate governance issues. In this context it co-founded the World Economic Forum's Partnering against Corruption Initiative and was central to the creation of the anti-money laundering standard of the Wolfsberg Group.

The Institute's International Center for Asset Recovery (ICAR) founded in July 2006 assists authorities in enhancing their capacities to seize, confiscate and recover the proceeds of corruption and money laundering. For this purpose, the ICAR trains officials in theoretical and strategic case assistance and facilitates co-operation between law enforcement agencies of different jurisdictions. In support of these activities, the ICAR operates a web-based knowledge-sharing and training tool, the Asset Recovery Knowledge Centre (www.assetrecovery.org)

Basel Institute on Governance
International Centre for Asset Recovery
Steinenring 60, 4051 Basel, Switzerland
Phone +41 61 205 55 11, Fax +41 61 205 55 19
www.baselgovernance.org, info@baselgovernance.org

Acknowledgements

We would like to extend our warm appreciation to the authors for their expert contributions, kindly submitted at short notice. Without their willingness to accept a tight deadline, this handbook would not have been completed in time for the Conference of the State Parties to the United Nations Convention against Corruption in November 2009 in Doha, Qatar.

This handbook draws together the combined skills and experience of practitioners in the field of asset tracing, creating a platform for knowledge sharing and capacity building. The enthusiasm with which the various authors have shared their experience and expertise is a credit to their commitment and dedication in this particular field of endeavour.

Many individuals contributed to the compilation of this handbook. In particular, Phyllis Atkinson for the Basel Institute on Governance's International Centre for Asset Recovery (ICAR) deserves special mention and a word of thanks as she bore responsibility for the general oversight, editing and co-ordination of the publication. Also worthy of mention are Nina Schild, Katrin Aegler, Daniela Winkler, Peter Huppertz and Anja Roth for ICAR whose contribution to the co-ordination of drafts, formatting and graphic design played a significant role in the successful completion of this handbook.

ICAR would not be able to operate without critical seed funding from the Swiss Agency for Development and Co-operation (SDC), the Government of Liechtenstein and the United Kingdom's Department for International Development (DFID). We remain grateful to our funders for their financial support which enables us to undertake a publication of this nature, among many other projects of equal significance to asset tracing.

Daniel Thelesklaf

Anne Lugon-Moulin

Basel Institute on Governance

List of Acronyms and Abbreviations

AML	Anti-Money Laundering
Anajembas	Christian and Amaka Anajemba
Anti-Bribery Convention	Convention on Combating Bribery of Foreign Public Officials in International Transactions
AR	Asset Recovery
Asnanis	Shamdas and Naresh Asnani
AU	African Union
AU Convention	African Union Convention on Preventing and Combating Corruption
BSA	Bank Secrecy Act
C	Claimant Victim(s) of the Fraud or Corruption
CFO	Chief Financial Officer
CI	Corporate Intelligence
CMS	Case Management System
CoE	Council of Europe
CoSP	Conference of State Parties
CSP	Corporate Service Provider
CTR	Currency Transaction Report
D	Defendant Perpetrator(s)
DFID	Department for International Development
DNFBPs	Designated Non-Financial Businesses and Professions
EFCC	Economic and Financial Crimes Commission
Egmont Group	Egmont Group of Financial Intelligence Units
EU	European Union
FATF	Financial Action Task Force
FinCEN	Financial Crimes Enforcement Network
FIU	Financial Intelligence Unit
IALEIA	Association of Law Enforcement Intelligence Analysts
IBC	International Business Cooperation
ICAR	International Center for Asset Recovery at the Basel Institute on Governance
ICT	Information and Communication Technology
ID	Citizens' Identification
IT	Information Technology
JIT	Joint Investigation Team

LSE	London School of Economics
MLA	Mutual Legal Assistance
Mr Alamieyeseigha	Diepreye Alamieyeseigha
Mr Chiluba	Frederick Chiluba
Mr Mobutu	Mobutu Sese Seko
Mr Nwandu	Chief Ezuge Nwandu
Mr Nwude	Emmanuel Odinigwe Nwude
Mr Rautenbach	Billie Rautenbach
Mr Sacaguchi	Nelson Sakaguchi
Mr White	Brian White
Mr Zakharov	Oleg Zakharov
NIL	Negotiable Instruments Log
NLP	Natural Language Processing
OAS	Organisation of American States
OCR	Optical Character Recognition
OECD	Organisation for Economic Cooperation and Development
OFAC	Office for Foreign Asset Control
PEP	Politically Exposed Person
POCA	Prevention of Organised Crime Act (South Africa)
RICO	Racketeering Influenced Corrupt Organisations Act
SADC	Southern African Development Community
SAR	Suspicious Activity Report
SOCA	Serious Organised Crime Agency (United Kingdom)
StAR	Stolen Assets Recovery Initiative
STR	Suspicious Transactions Report
T	Third Party Accomplices
UK	United Kingdom
UNCAC	United Nations Convention against Corruption
UNODC	United Nations Office on Drugs and Crime
UNTOC	United Nations Convention on Transnational Organised Crime
US	United States of America
1988 Vienna Convention	United Nations Convention against Illicit Trafficking in Drugs and Psychotropic Substances

PHYLLIS ATKINSON*

Introduction

Corruption generates billions of dollars each year. A large portion of the assets acquired through acts of corruption can never be recovered by victim countries for the simple reason: it was not possible to locate them. Corrupt officials and bribe payers, often multi-national companies, frequently use the opportunities presented by financial services providers and so-called 'gatekeepers' to conceal and enjoy the proceeds of their unlawful activities. Today's financial centres – the cities where big financial transactions are done and an array of financial products are traded – include not only long-established places such as New York, London and Tokyo but also a growing number of newer financial hubs in Asia, the Middle East and beyond. The profits generated by crime are often transferred to financial centres in an attempt to thwart or complicate efforts by law enforcement agencies to identify and trace assets acquired in the process. The success of public corruption, money laundering and most financial crime investigations, therefore, depends largely upon the criminal investigator's ability to track the ownership trail of money and other assets.

Proceeds of crime represent criminal income. They manifest themselves as assets, some of which are the object of the crime itself, such as stolen funds. However, in more complex financial crimes, the asset to be linked to the offence is more likely to be the product of an intervening transaction and is in a fungible form. Tracing the proceeds of crime is premised on the assumption that through transformation, the origin of assets as criminal income can be concealed, and they can be easily and speedily moved between locations, or across borders. They can be mingled with others and converted into other forms.

To benefit from profit-generating crime, criminals are usually forced to launder the proceeds to hide the origins thereof. If the investigator knows how and where to look, there is always a connection between criminals' assets and their crimes. In addition to often providing evidence of criminal intent and identifying otherwise unknown accomplices, tracking the ownership trail may also lead to the seizure of property constituting illegal proceeds. To trace money and property successfully, the investigator must be equipped to uncover and identify ownership interests often camouflaged by changes in the form and nature of the ownership, and know how to unravel accurately cleverly disguised control over, and interest in, property. He or she must also know who to approach for information, where such information can be found, what can be used to create a financial profile and how to manage the collated information in the most efficient and effective manner.

Integrated financial investigation is an essential element of any strategy for targeting proceeds from crime. The investigative process is the core activity, forming the basis for any asset recovery effort, asset recovery (particularly at an international level) involving an overlapping of anti-corruption, anti-money laundering and broader law enforcement agendas. A jurisdiction where funds have been secreted will not confiscate or repatriate the assets to the country of origin unless evidence is presented, linking them to an illegal activity. This evidence must, furthermore, be admissible in

* Phyllis Atkinson, a lawyer by profession and former prosecutor/advocate in South Africa for 23 years, is a Senior Asset Recovery Specialist with the International Centre for Asset Recovery (ICAR) at the Basel Institute on Governance in Switzerland.

court proceedings. As a preliminary activity to the recovery of stolen assets, the identification and tracing of the proceeds of crime and securing the property for final confiscation is an essential part of the process. This is a demanding task which should be conducted in parallel with the investigation of the criminal offence generating material benefit. It requires intense cooperation between law enforcement agencies or those tasked with tracing assets, Financial Intelligence Units and, in most instances, the prosecutor. Where an investigation focuses, for example, on a public official's receipt of bribes or otherwise unlawful financial enrichment, this will require the involvement of investigators experienced in gathering and analysing financial evidence. In many instances, it will also require the involvement of a forensic accounting expert to assist in unraveling complex financial transactions, and an understanding of the role played by gatekeepers in assisting (sometimes unwittingly) criminals dispose of their criminal profits.

In many countries, criminal investigations are primarily directed towards the investigation of the underlying criminality. It is still comparatively rare for investigators, as a routine part of the investigation of major proceeds-generating offences, to '*follow the money*' and establish what happened to the proceeds. Such investigations undoubtedly need resources, expertise and, almost inevitably, effective international cooperation. Securing evidence abroad often provides the key to success in a complex, commercial investigation or those involving other forms of serious crime, and results in the successful recovery of assets. In many instances, it also results in the successful prosecution of those involved in organised crime.

This unique publication aims to provide practical guidance to the practitioner. In so doing, it is recognised that the process which leads to recovery or the repatriation of assets, is divided into four (4) basic phases, i.e.,

- Pre-investigative phase, during which the investigator verifies the source of the information initiating the investigation and determines its authenticity. If there are inconsistencies in the story or incorrect statements and assumptions, then the true facts must be established
- Investigative phase, where the proceeds of crime are identified and located and evidence in respect of ownership is collated covering several areas of investigative work in the process, for example, Mutual Legal Assistance requests to obtain information relating to offshore bank and other records, and financial investigations to obtain and analyse bank records. The result of this investigation can be a temporary measure (seizure) to secure later confiscation ordered by the court
- Judicial phase, where the accused person/defendant is convicted (or acquitted) and the decision on confiscation is final
- Disposal phase, where the property is actually confiscated and disposed of by the State in accordance with the law, whilst taking into account international asset sharing

It is recognised that the stages in the asset recovery process include the lead or pre-lead (or intelligence) which triggers the investigative process aimed at tracing the assets and collating evidence in support of the criminal investigation. The freezing and seizure stages fall largely under the auspices of the judicial system. Finally, the seized assets are returned to the requesting country.

It is not, however, the intention of this handbook to deal exhaustively with the entire process in terms of which assets are ultimately forfeited or confiscated. The purpose of this handbook is to provide guidance to the investigator to the point where judicial proceedings aimed at the forfeiture or confiscation of the proceeds of crime may be instituted. In addition to covering the pre-investigative and investigative stages during

which information is collated and verified and assets are identified and located, it also provides guidance aimed at the freezing or seizure of assets. This often becomes a necessity during the tracing phase, and is a reference to the process in terms of which the transfer, destruction, conversion, disposition or movement of property or assets is temporarily prohibited, or custody or control of property is temporarily assumed on the basis of an order issued by a court or other competent authority.

In order to facilitate a final confiscation, it is necessary to develop efficient investigative and provisional methods to:

- Identify
- Trace
- Freeze or seize rapidly property which is liable to confiscation in order to prevent any dealing in, transfer or disposal of such property and facilitate the confiscation at a later stage

Although this handbook does not purport to cover all such investigative and provisional methods, it does highlight some of the major steps an investigator needs to take in order to ensure a thorough and effective asset tracing investigation.

Information and Communication Technology (ICT) and case management play a crucial role in the criminalisation of corruption and implementation of a process or system to detect, investigate and prosecute serious cases of corruption, money laundering and other financial crimes. They play an equally important role during the investigation process aimed more specifically at tracing and recovering assets. Increasingly, the investigative process of corruption cases, inclusive of asset tracing, involves the collation and analysis of large volumes of data. During the financial investigation which inevitably arises as a result of this process, a good ICT tool is imperative. Without an ICT system, the financial investigator will be looking for the proverbial 'needle in a haystack'.

Lawyers, financial advisors, notaries, accountants and other similar professionals (the so-called 'gatekeepers') are increasingly used in cases where criminals seek to conceal their ill-gotten gains as they are well-placed to facilitate money laundering and the concealment of assets generally due to their knowledge and expertise. This, in turn, requires the investigator to gain an understanding of the types of assistance provided by such professionals, being the gateway through which criminals often pass to achieve their objectives, for example, the creation of corporate vehicles or other complex legal arrangements such as trusts. He or she also needs to understand the manner in which the secrecy offered by legal privilege is exploited, the veneer of respectability is obtained by engaging their services and how corporate vehicles are manipulated and misused in the process.

Banking institutions act as obvious gatekeepers for the legitimate financial system. It is usually through their vigilance that the system can be protected from providing organised crime syndicates or terrorists with the mechanism for concealing the proceeds of illicit and corrupt activity. Although they play a crucial role in the prevention, detection and reporting of money laundering, there is an increasing focus on non-banking and even non-financial institutions as they too are used by money launderers, seeking to invent ingenious means of enjoying their ill-gotten gains.

Persons and/or entities other than banking institutions such as legal professionals, auditors, accountants, tax advisors, insurers and estate agents, have, in many ways, moved to 'centre stage' in the fight against money laundering, both globally and locally.

Cross border criminal activities demand international cooperation during the investigation and proceedings aimed ultimately at the confiscation of the proceeds of

crime. International cooperation should facilitate the provision of investigative assistance in identifying and tracing property, obtaining documents and enforcing provisional measures aimed at freezing or seizing the proceeds of crime. Knowing how to approach an investigation with a transnational component is a vital tool in the toolkit of any investigator tasked with tracing assets.

The current international Anti-Money Laundering framework consists of a number of elements of relevance to asset tracing, e.g., the due diligence measures for financial institutions and designated non-financial businesses and professions. Each of these elements should be given due consideration with a view to identifying potential for use by investigators in tracing stolen assets, and are duly covered by this publication.

In conclusion, this publication presents practitioners' views on how assets generated by corruptive acts can be traced, located and finally frozen. It covers some of the challenges an investigator can expect to encounter when embarking on an asset tracing investigation. It also comprises examples of successful cases, and provides for practical assistance to investigators (mainly in developing countries) with the focus being on assisting developing countries trace assets concealed in financial centres. Given the fact that many investigations which involve asset tracing focus on fraud as the underlying predicate offence, lessons to be learnt in this regard have been included in this handbook: for example, key civil interim measures and remedies available from the English civil court for securing recoveries for a victim of fraud (and corruption or other acquisitive crime) are covered as these remedies are regarded as the lawyers' 'Nuclear Weapons' and provide invaluable assistance to the investigator of corruption matters. Properly applied for and used, freezing property and search orders can put the claimant in the strongest possible position on day one of the proceedings to trace, secure and recover the proceeds of the claim or fraud (or corruption) upon him, however that crime has been perpetrated.

CHARLES GOREDEMA*

Recovery of proceeds of crime: observations on practical challenges in sub-Saharan Africa

I. Introduction

Proceeds of economic crime comprise the following:

> 'Property derived or realised directly or indirectly from a (serious) crime, (the initial criminal proceeds) and includes property resulting from the conversion or transformation of the initial criminal proceeds (secondary criminal proceeds) and income, capital or other economic gains derived from either the initial criminal or the secondary criminal proceeds.'[1]

Numerous forms of predatory crimes yield proceeds, in the form of assets, some of which are the object of the crime itself, while others are the result of intervening transactions that may conceal the connection to the crime. Initial proceeds can be mingled with others and converted into secondary forms. Furthermore, criminal assets can be speedily moved between places, or across borders. This often complicates the task of identifying proceeds of crime for the victim or for any other claimant, and is a basic challenge in this area.

This chapter examines recurrent hurdles which make the recovery of proceeds of crime an enduring issue in the contemporary implementation of criminal justice and economic policy. It explores them from the standpoint of both the victim/claimant in a predatory crime situation and an investigator/prosecutor acting in a representative capacity.

In his book *Accounting Guide to Asset Tracing*, Dave Melton defines asset tracing in the context of divorce proceedings as

> 'an accounting process that traces an asset from its separate property beginnings through all of its mutations and demonstrates that the resulting asset in existence at the date of divorce is either separate, marital, or a combination of the two.'[2]

The definition can be adapted for investigative processes into proceeds of crimes, such as fraud, drug trafficking, money laundering and corruption. Tracing proceeds of crime involves identifying assets with or from their criminal origins, through all mutations, if any, to the eventual form and state in which they exist at the time they are located. During mutation, proceeds mingle with lawfully accrued resources and can diminish or grow in quantity or appreciate in value.

---

* Charles Goredema heads the Organised Crime and Money Laundering Programme at the Institute for Security Studies in Cape Town, South Africa. He has been involved in research and networking in the formulation of responses to economic crime and money laundering over the past 10 years.

1 This definition is paraphrased from several criminal statutes, including the Serious Offences (Confiscation of Proceeds) Act (Zimbabwe) and the Prevention of Money Laundering Bill (Malawi).

2 Chapter 1 of the book can be accessed at www.assettracing.com/book/tchp1.htm (accessed on 18 October 2005).

In a joint report to launch the Stolen Assets Recovery Initiative in 2007[3], the United Nations Office on Drugs and Crime (UNODC) and the World Bank summed up the formidable challenges still encountered in locating and retrieving proceeds of crime. This is particularly so where proceeds of corruption by political and economic elites are involved, or where the proceeds have been moved across borders. State responses to corruption, and to the transnational movement of proceeds of crime are not always easy to activate or coordinate.

Policy makers and law enforcement agencies are aware that tracing the proceeds of crime, whether the crimes are organised or not, predatory or market-based, can be stifled by money laundering techniques. This is, at least, part of the reason for the ascendancy of anti-money laundering measures up the scale of global priority issues. Since the advent of the United Nations Convention against Narcotics and Psychotropic Substances (1988), measures to detect and retrieve proceeds of crime have been accorded prominence. The emphasis was repeated for a broader range of crimes in the United Nations Convention against Transnational Organised Crime (2000). The regional Southern African Development Community (SADC) Protocol Against Corruption (2001) adopted this approach for proceeds of corruption, as did the African Union Convention on Preventing and Combating Corruption and Related Activities: (2003) and the United Nations Convention against Corruption (UNCAC) (2003).

The role of confiscation regimes in anti-money laundering mechanisms is also not questionable. At the same time, the attention devoted to effective strategies and laws to trace proceeds of crime in sub-Saharan Africa is still inadequate. This chapter discusses some of the key challenges in establishing effective systems, and highlights the manner in which these challenges manifest themselves in the daily experiences of the victim or investigator. It argues that some of the most persistent challenges are policy-related. The final section points to some milestones that have been achieved in the sub-region and elsewhere, with a view to drawing lessons for the evolution of this aspect of combating economic crime.

II. Who has an interest in tracing and retrieving the proceeds of crime?

The nature, magnitude and perhaps the way in which criminal income integrates into the economy, depend on the nature of the crime from which it is derived. Economic crime analysts draw a distinction between predatory crime and market-based (or related) crime. The categorisation is admittedly woven around stereotypes but it is useful. At its simplest, predatory crime involves:

> 'the redistribution of existing wealth. The transfers are bilateral, involving victim and perpetrator… (and) the transfers are involuntary, commonly using force or the threat of force, although deceit may suffice. The victims (individuals, institutions or corporations) are readily identifiable. The losses are also simple to determine – a robbed (or defrauded) person, institution or corporation can point to specific money and property lost.'[4]

Classic instances of predatory crime are robbery and fraud. The victims of predatory crime are usually, but not always readily identifiable. Cases of grand corruption occasionally raise victim-identification challenges.

3 The report is accessible on the website of the World Bank at www.worldbank.org.
4 R T Naylor (2002), *Wages of crime*, Cornell University Press, 252–3.

Market-based crimes, on the other hand:

> 'involve the production and distribution of new goods and services that happen to be illegal by their very nature. The exchanges are multilateral, much like legitimate market transactions, involving (among others) producers, distributors, retailers and money managers on the supply side and final consumers on the demand side. Because the transfers are voluntary, it is often difficult to define a victim, unless it is some abstract construct like 'society'. Therefore, there are no definable losses to any individual from the act itself (although there may be from indirect consequences of the act…).'[5]

Against that background, it is necessary to determine who has an interest in detecting and recovering the proceeds of crime. On that determination may depend the subsequent processes pursued, the difficulties that may arise, and the prospects of success.

In predatory crime, the victim of the crime will typically be anxious to get compensation. The interest of the victim may be shared, or pursued on their behalf, by prosecutors, forensic investigators, accountants, anti-corruption agencies, anti-money laundering investigators and the courts.

For market-based crimes, the absence of direct victims means that the keenest interest to uncover connections between the crime and its proceeds is held by one mandated agency or another. The latter is mandated to represent the public, or the state, or even 'society' or a section of society. There may be a multiplicity of institutions with this role, or that perceive themselves to have it. They may include police departments, taxation authorities, asset forfeiture agencies, intelligence agencies and banks. Such 'victims' may be classified as representative victims. Whether they can effectively act to recover the proceeds ultimately depends on their capacity – which, in turn, is centred around the extent to which their role is recognised and supported by law.

While it cannot eliminate all of the hurdles, the backing of the law can ease the processes involved in finding proceeds of crime, regardless of whether the victims are actual or representative.

One notable deficiency of legal systems in sub-Saharan Africa is evident with respect to predatory crimes such as grand corruption, or market-based crimes such as commodity trafficking. It is the failure of states to resolve debilitating contests for the leadership of asset recovery initiatives. The predominant position appears to be the one inherited by most common law countries, where the Attorney-General, as head of the prosecution, is vested with the leading role. This is often an exclusive role. With the appropriation of many Attorneys-General by political elites that may be implicated in corruption, there is much pressure to move away from the inherited position. Various alternative models on leadership are emerging but much friction is evident.[6] Cooperation, where it exists, tends to depend on personalities rather than institutionalised relationships. In the last few years, many countries have been working on harmonising strategies against corruption and money laundering. The process is incomplete. While it is occurring, a framework to foster collaboration among the agencies with an interest in the recovery of proceeds of crime is needed.

The risk of disparate agencies sabotaging each other is real. In some countries, the value of recovered assets is 'credited' to the recovering agency. At the end of a given year, the credits may impact on financial rewards to officials. This is intended to create

5 Ibid.

6 This was highlighted in Zambia in August 2009, following the acquittal of the former President, F Chiluba on corruption charges. The head of the task force that had investigated the case indicated that the task force would appeal against the decision. The Attorney General disagreed, resulting in the dismissal of the task force head.

an incentive for industry but it could also motivate officials to be secretive about ongoing investigations and to withhold information from colleagues in other institutions.

III. What are the challenges to retrieval of the proceeds of crime?

It is difficult to identify issues that are solely peculiar to tracing and retrieval of the proceeds of crime and do not arise in relation to other aspects of economic crime. Whether the crime is predatory or market-based, the proceeds are likely to have been concealed from public view, either physically or by tampering with documentation constituting the paper trail. Money laundering is intended to conceal the proceeds of crime by various methods. Conventional measures to combat money laundering rely on the identification of the most common methods and the avenues used. As these measures expand in scope and coverage, so apparently do the innovative concealment mechanisms. Responses to money laundering tend to lag behind typologies of money laundering.

One of the reasons for the adoption of a new asset confiscation regime in the Proceeds of Crime Act (2002) in England and Wales was the low level of recovery of proceeds of crime. Levi (2003) has attributed this deficiency to several factors, all related to capacity. They are just as relevant to Africa. He asserts that failure was due to:

- Moderate investigative knowledge, due to the inherent secrecy of the activities and inadequate resource allocation to financial aspects of crime
- Inadequate co-ordination and intelligence exchange between police and the revenue department, due partly to legislative prohibitions on data sharing but also reflecting differences in cultural and policy objectives
- Inadequate use made of suspicious transaction reports by the police and customs agencies due to a lack of resources and the inherent difficulty of following up many reports without contacting the accountholder for an explanation
- Inadequate powers to detain cash of unexplained origin other than drugs money at borders.7

These shortcomings pertain to law enforcement agencies, or representative victims. They would be even worse in respect of personal victims, as they do not have the necessary capacity to investigate complex crime or the backing of public infrastructure. There is no legal system in Africa that entitles a victim or non-state investigator to invoke the investigative authority of public law enforcement structures, or to compel private repositories of information to disclose such information.

The tendency of criminals to transfer illegal income across borders is well known. This is usually the case when such income is derived from a weak economy, and is even more likely if the income can be converted to a stronger currency acceptable in the destination country. The asset portfolio attributed to resource plunders by the likes of Mobutu Sese Seko (Mr Mobutu) in Zaire illustrates this. Russell notes that:

7 Michael Levi (2003), 'Criminal Asset Stripping' in A Edwards and P Gill (editors), *Transnational Organised Crime: Perspectives on Global Security*, 212-26.

> 'His property constellation included a vineyard in Portugal, a thirty-two room mansion in Switzerland, a castle in Spain and a magnificent first floor apartment in Paris close to the Arc de Triomphe and within easy walking distance of the furrier who made his leopard-skin hats. The piece de resistance was his marble palace in his home village, Gbadolite.'[8]

While the inclination to move proceeds of crime abroad is established and relatively well publicised, less well-known are the routes of transfer between countries and regions. Even less well-known are the precise ways by which such income is infiltrated into the country of destination. Anecdotal observations in Southern Africa show the following:

- That the mode chosen by which to infiltrate proceeds depends on the structural weaknesses identified in the host country, such as the demand for foreign investment
- If record keeping of transactions involving incoming foreign currency is poor or non-existent this will be an incentive

These features affect the risk of detection of illegal income on its entry into the socio-economic environment, technically described in money laundering as placement of illegal income (but which could also be integration of illegal income with legitimate income), or as it mutates within it, a stage referred to in money laundering as layering. A country with no vigilant anti-money laundering regime is likely to have an environment that does not support the tracing and recovery of proceeds of crime of foreign origin.

The range of underlying criminal activities from which laundered funds are derived is broad and continually expanding. Illegal income does not have a homogeneous source. It may start off as legitimate income, as is the case with proceeds of tax evasion, or misappropriated funds. There is always potential for ambivalence in the way different jurisdictions regard funds acquired in 'questionable' circumstances. In Southern Africa, the utility of controls on the movement of foreign exchange across borders is often called into question.[9] Bulk movement of currency, predominantly involving the exchangeable currencies, is prevalent. The countries which encounter frequent movement of foreign exchange across borders include Angola, Namibia, South Africa, Zimbabwe, Lesotho, Tanzania and Malawi. There is also evidence of bulk cash movements between southern African countries and China. There is hardly any evidence of the scrutiny of the source of funds emanating from one country as they are transferred across borders.

Informal economies in the sub-region are vast, with the result that funds smuggled out of one country can be kept and used outside the banking system of the destination country by the smuggler, or anyone else for that matter. They can be used to purchase an asset, which is smuggled to the country from which the funds came. The seller can re-smuggle the purchase price to a third country and invest them in, say, real estate. The frequency with which transactions of this nature occur between South Africa and its neighbours is a matter of speculation but their occurrence is well known. Once in the destination country, proceeds can be invested in securities, which are more difficult to trace and far easier to dispose of than real estate.

Among the primary challenges to the recovery of the proceeds of crime is the lack (or in some cases, slow pace) of exchange of crime intelligence among the affected countries. This deficiency affects proceeds of both activities which are universally

8 Alec Russell (2000), *Big men, little people: Encounters in Africa*, Pan Books, London, 18.

9 The Common Monetary Area pact, which binds South Africa, Swaziland, Lesotho and Namibia, purports to restrict the transmission of cash across member states' borders to R 10,000 per crossing. In reality, there is no enforcement of the prohibition and the limit is frequently violated.

regarded as criminal and activities whose criminality is a matter of controversy. Transnational mechanisms to track movements of assets between countries are passive rather than pro-active. Whether criminal money will attract the attention of the host country's authorities depends more on whether they have been alerted to its presence by the source country than on the host country's own vigilance.

The appreciation of the victim that an offence has been committed is as much a critical factor as is their determination to obtain compensation. There is no mechanism to take up cases on behalf of victims of predatory crime without their initiative and involvement. Crimes are sometimes categorised as 'victimless' simply because of victim ignorance. The plunder of the economies in Zaire (under Mr Mobutu), Nigeria (under various military generals) and Zambia (under Frederick Chiluba) were committed without the knowledge of the large sections of the public in those countries. In illicitly enriching themselves, corrupt political and economic elites almost always elude the tax authorities,[10] who might be expected to play a gate-keeping role. The citizens, who are the ultimate victims, often only become aware of the corrupt acts long after their commission, at a time when the proceeds have been moved across many borders. It is still commonplace in the region for investigative commissions of inquiry to report their findings in secret, and for the reports to be kept away from the public. The recommendations of commissions established in recent years to investigate fraud and corruption cases in Namibia, Zimbabwe, Uganda and Kenya have not been implemented.

Recovery of the proceeds of crime broadens the discussion beyond the sub-region. Even if one were to take no account of globalisation, one would still have to recognise the historical, trade and economic connections between much of Africa and the developed economies of Western Europe and the United States, and emerging economic giants like China, Brazil and India. The most notorious criminals of Africa, including politicians, have always taken advantage of the bonds bequeathed by colonial history. As Scher puts it, perhaps more than any other sphere of transnational relations, the repatriation of assets dishonestly acquired in developing source countries and transferred to developed countries is

> 'fraught with the complicity of the banks involved, the navigation of a costly international legal labyrinth and the fact that those most implicated in public looting usually have the most power and influence.'[11]

While there is no estimate of the scale of proceeds of unlawful activity transferred between the sub-region and Western Europe, the anecdotal indicators point towards significant movements. Declarations by applicants for tax and exchange control amnesty in South Africa for funds unlawfully invested outside the country reflected that just over R 68 billion (more than USD 8 billion) was involved, with most of it in western European economies. Virtually all the proceeds of Mr Mobutu's corruption that were transferred abroad ended up in Western Europe, primarily Belgium and France. In the absence of investigation, no one can assert with certainty that there was complicity on the part of the receiving countries or institutions. One can, however, assume with greater confidence that banking confidentiality in the destination countries ensured that a substantial part of the externalised proceeds remained out of the sight of national authorities in the source countries. A combination of such

10 Reference may be made to the exploits of politicians reported in the October 22 issue of the Zimbabwe Independent on illicit dealings with hunting concessions and game lodges on farms acquired under the so-called land reform programme in Zimbabwe.

11 Daniel Scher, in an article published in the African Security Review, 2005, 14:4, under the title 'Asset recovery: Repatriating Africa's looted billions', 17.

confidentiality and victim country inaction has occasionally been to blame for some of the intractable crime proceeds cases.

In a paper presented at the International Bar Association Annual Conference in Prague in 2005, Gully-Hart explored the problems that affect the recovery of proceeds of grand corruption that may have ended up in Switzerland.[12]

The first challenge emanates from the immunity that is normally vested in heads of state from the processes of criminal and civil law. Examples of kleptocrats who exploited immunity to loot national coffers abound.[13] The second is attributable to the failure of the victim state to initiate domestic proceedings, or, having initiated them, to conclude them. Legal assistance proceedings to recover the Mobutu assets commenced in 1997 but remain incomplete to date. Swiss authorities have attributed the lack of progress to absence of movement from the Democratic Republic of the Congo. The same has occurred in respect of assets linked to Jean-Claude Duvalier. Thirdly, the problem could emanate from non-compliance with certain minimum conditions stipulated by the systems of the receiving state, in this case, Swiss law. Gully-Hart asserted these conditions to be:

- That the victim country had to show that it observes standards of fair trial
- Dual criminality, that is to say that activity from which the assets were derived is recognised as a crime in Switzerland, and
- That the assets in question are probably proceeds of the crime. The victim state carries a responsibility to show the link between proceeds and criminal activity on a balance of probabilities

The Convention seeks to do away with the requirement of dual criminality as a pre-condition for mutual cooperation among state parties.

The fourth challenge relates even more directly to the way that the requesting country is perceived by the requested country. If it is perceived to be corrupt and lacking good governance, that can be used as a basis for refusing repatriation. Since the judgment and the basis for it are for the requested country to make, the process is susceptible to subjective considerations.

Finally, repatriation can be stalled by the contradictory claims of third parties that claim to be innocent of the underlying crime.

---

12 Paul Gully-Hart presented a paper to the Anti-Corruption Working Group entitled 'Grand Corruption and the repatriation of looted funds: the position in Switzerland'. The key legal and practical difficulties are outlined on pages 6-7.

13 Below is a summary of the best-known cases.

Head of State		
Sani Abacha	Nigeria	USD 4.3 billionn
Felix Houphouet	Ivory Coast	USD 3.5 billion
Ibrahim Babangida	Nigeria	USD 3.0 billion
Mobutu Sese Seko	Zaire	USD 2.2 billion
Moussa Traore	Mali	USD 1.8 billion
Henri Konan Bedie	Ivory Coast	USD 200 million
Denis Sassou Nguesso	Congo	USD 120 million
Omar Bongo	Gabon	USD 50 million
Paul Biya	Cameroon	USD 45 million
Haile Mariam	Ethiopia	USD 20 million
Hissane Habre	Chad	USD 2 million

Source: www.antimoneylaundering.ukf.net/papers/jbrooks.ppt

Any survey of the prospects of asset recovery should consider the legal and practical issues that impede or slow down asset repatriation. They emanate from both domestic and foreign realities. In a number of countries, the source of the problem is the manner in which the agencies and institutions at the coalface of crime intelligence gathering are organised. Typically, they comprise the police, security intelligence agencies, customs and taxation departments and anti-corruption agencies. A survey of the sub-region reveals how thin the field is in terms of institutions dedicated to tracking the proceeds of crime. A dedicated Asset Forfeiture Unit was established in the wake of the Prevention of Organised Crime Act (1998) in South Africa. A similar structure was set up in Namibia in 2008 but there do not appear to be similar structures anywhere else in the sub-region.

Each of the various law enforcement agencies gathers intelligence and experience of value to asset tracing and retrieval. The fragmentation and the absence of a framework for cooperation limits the scope for synthesis of effort. Sometimes, there are rules against information sharing among the agencies.[14] Occasionally, conflicts over operational territory and tactics degenerate into hostile bickering and infighting. South Africa's erstwhile Directorate of Special Operations (otherwise known as the Scorpions) was occasionally entangled in controversy in the latter years of its existence, stemming from a problematic working relationship with the police service, on one hand, and intelligence agencies on the other.[15] The resulting conflict impeded crime detection in general and the pursuit of the proceeds of crime in particular.

In some countries, it is not the only kind of conflict encountered. In designing an effective system to recover proceeds of crime, what appears is a conceptual conflict between pursuing proceeds as part of enforcing criminal justice or treating it as an instrument of economic policy. Addressing the issue is critical partly on account of the ethical ramifications of opting for one approach or the other. The connection between illegal assets and the crime from which they were derived makes it difficult to conceive that their recovery can ever be regulated differently to the determination of guilt or innocence of the alleged criminal. This obviously renders the efficiency and effectiveness of the recovery regime dependent on the efficiency of the rest of the criminal justice process. In turn, this means that the fewer the number of convictions in economic crime cases, the smaller the level of recoveries.

A system that is mired in economic justice, on the other hand, is more likely to recognise that organised crime and corruption, as well as the myriad other sources of criminal income, cannot be confronted only by the criminal justice system. The process of detecting and recovering criminal income is complementary to but distinguishable from the rest of the criminal justice process, especially from the criminal trial. The goals are to bring criminal income into the legitimate mainstream, if it is circulating outside. If criminal income has already penetrated the legitimate economy, the objective becomes to remove it from the possession or control of the suspect beneficiary, even though he/she may never be convicted of any crime. Asset seizure as an instrument of economic justice will easily use amnesties and taxation measures to mop up illicit income. The tax and exchange control amnesty may be regarded as a relatively controversy-free process or uncovering proceeds of crime.

Retrieving proceeds of crime can serve other policy objectives. Among them are economic policy aspirations, such as:

- Drawing illegally acquired funds into the public financial system

14 In one country, for instance, certain information collected by revenue authorities cannot be disclosed to crime intelligence.

15 The conflict is receiving publicity as the hearings of the Kampepe Commission progress. See the South African Sunday Times newspaper, 23 October 2005.

- Collecting unpaid taxes and
- Combating unlawful enrichment and thereby reinforcing the moral lesson that crime does not pay

This, however, requires dealing with the potential for disharmony between the agencies responsible for enforcing criminal justice and agencies enforcing economic policy concerns. Compromises may be required from time to time. Accordingly, it is necessary to forge a mechanism by which to determine which objectives to push to the front and which to sacrifice.[16]

More controversial in the sub-region have been efforts to adopt civil forfeiture, enabling confiscation without conviction, along the lines of the Racketeer Influenced Corrupt Organisations (RICO) Act in the United States. While the more draconian dimensions of RICO have not really found favour, some of its features have been adopted, notably in South Africa. The Prevention of Organised Crime Act (1998), which is often called POCA, enables the state to secure the confiscation of assets belonging to a person not convicted of any crime. The state needs to show that the assets are probably proceeds of crime, considering all relevant factors. The confiscation process can take place before or after the criminal trial. Civil forfeiture has proved quite useful in the case of fugitives from justice, such as Billy Rautenbach.

UNCAC, which became effective in December 2005, does not directly prescribe civil forfeiture as a method of retrieving proceeds of crime but it advocates measures that create a conducive environment for civil forfeiture. The Convention stipulates for a pro-active system of due diligence, information documenting and suspicious activity reporting, which, if implemented, can make it easier for agencies tasked with civil forfeiture to discharge their obligations.

Article 14 sets out a framework for measures against the concealment of proceeds of crime through money laundering techniques. It is complemented by the provisions of Chapter V on asset recovery. Article 51 captures the general thrust of Chapter V, thus:

> 'the return of assets pursuant to this chapter is a fundamental principle of this Convention, and State parties shall afford one another the widest measure of co-operation and assistance in this regard.'

Implementation of the Convention will probably depend on effective agencies against corruption. The Convention is discussed further below.

IV. Challenges connected to mutual legal assistance

An anti-money laundering structure without the capacity to track proceeds of crime is incomplete. As indicated above, there should be clarity as to the mandate to follow up and seize proceeds of crime, as well as clarity on the structure is to be funded. It should also be clear as to who has authority to seek, or extend, cooperation with foreign institutions. The connection between money laundering and predicate criminal activities potentially brings the police, anti-corruption agencies and the public prosecution into close proximity in what should be an integrated or collaborative law enforcement network.

16 In South Africa, a Ministerial Coordinating Committee is created in the National Prosecuting Authority Act (1998). The Minister of Justice convenes the committee. Indications are that it has not been functioning as intended.

International cooperation raises three related elements of relevance to this study, namely mutual legal assistance, the repatriation of proceeds of crime/corruption and extradition. Each has tended to be dogged by issues such as:

- Banking secrecy
- The insistence by some countries on dual criminality
- Slow pace of exchange of information between countries, partly because of protocol or differences in procedural systems between countries
- Costs

Countries with significant offshore banking and investment sectors, such as Switzerland, are regularly required to provide mutual assistance in investigations or asset repatriation. UNCAC has been praised as a vehicle to simplify this area of combating corruption and money laundering. Much can be learnt from experiences that developed before UNCAC, stemming from the Commonwealth Harare Scheme (1991) and the Organisation for Economic Community Development (OECD) Convention on Combating Bribery of Foreign Public Officials in International Business Transactions (1998). The SADC Protocol on Mutual Assistance in Criminal Matters (2002) is also an important instrument on which to rely.

International legislation to regulate mutual legal assistance in the absence of bilateral treaties provides mechanisms for international cooperation for signatory countries to utilise. It seeks to prevent banking secrecy being used to impede mutual legal assistance requests, (see Palermo Convention, UNCAC, the Financial Action Task Force (FATF) Recommendation 40) and to expedite processing of requests. Information exchange could be speeded up by the greater use of technology, and joint membership of the Egmont Group of financial intelligence units.

Costs are a more formidable challenge, in that they may be incurred by a country with no interest in the case. UNCAC prescribes some kind of formula, in terms of which the requested country is compensated for extraordinary expenses incurred in tracing, freezing, confiscating and returning assets. In this regard, it adopts a similar approach to the SADC Protocol. Dual criminality is not a mandatory ground for refusing to assist a requesting state.

V. Seizing and disposing of the proceeds of crime: the milestones

At the 11th Congress of the United Nations on Crime Prevention and the Rehabilitation of Offenders, it was reported that:

> '…since economic crimes, including money-laundering, are committed for the purpose of obtaining profit, tracing, freezing, seizing and confiscating the proceeds of crime are the most effective measures against those criminal activities. The latest sets of measures that the international community agreed to take can be found in the Organized Crime Convention and, more recently, in the United Nations Convention against Corruption, especially its chapter on asset recovery. There is an urgent need to enhance domestic and international efforts to further develop and utilize those measures to the full.'[17]

17 Working papers tabled at the workshop on measures to combat economic crime, including money laundering.

This part of the chapter highlights some of the experiences on which the sub-region can draw in the seizure and disposal of the proceeds of crime. The initial point is that asset tracing, seizure and disposal did not come into being on account of anti-money laundering.

Milestone 1: SADC Protocol against Corruption (2001)

Article 8 of the Protocol mandates each state party to adopt measures necessary to identify, trace, freeze, seize and eventually confiscate proceeds of corruption. Recognising that the proceeds of crime may be in the custody of financial intermediaries, the Protocol directs state parties to authorise courts and 'other competent authorities' to override bank secrecy in pursuing such proceeds.

It is evident that courts in all of Southern Africa can override the confidentiality between a bank and its customers. However, that position seems to have been in existence well before the advent of the Protocol.

The bank customer's right to confidentiality of information about him is a long recognised right at common law. In many countries, the right is embodied in statutes regulating the conduct of banking business. In fewer countries, the right to privacy is a constitutional right and therefore fundamental. In essence, the relationship between a bank and its customer is based on contract. An implicit term of the contract is that the bank should not disclose to third persons either the state of the customer's account, or any of his transactions with the bank or any information relating to the customer acquired through the maintenance and administration of the account. Non-disclosure is not absolute and may be infringed if a court so orders, or if disclosure is required for the bank's own protection, or to prevent fraud or other crime.[18] In the words of an eminent jurist:

> '...there must be important limitations upon the obligation of the bank not to divulge such information…It is plain that there is no privilege from disclosure enforced in the course of legal proceedings. But the bank is entitled to secure itself in respect of liabilities it incurs to the customer or the customer to it, and in respect of liabilities to third parties in (for) transactions it conducts for or with the customer. …the obligation not to disclose information...is subject to the qualification that the bank has the right to disclose such information, when, and to the extent to which it is reasonably necessary for the protection of the bank's interest, either as against their customer or as against third parties...or for protecting the bank or persons interested or the public against fraud or crime.'[19]

Milestone 2: The United Nations Convention against Corruption (UNCAC) and the African Union Convention on Preventing and Combating Corruption (AU Convention) of 2003

These two instruments can be considered together as a major development in getting a common position on repatriation of the proceeds of crime. UNCAC came into force at the end of 2005.[20] Article 57 provides a mechanism to repatriate the proceeds of, *inter alia*, corruption and embezzlement of public funds, to states that can establish legitimate entitlement.

18 See paragraph 240 of Halsbury's Laws of England (4th edition), Vol. 3 (1989); *Tournier v National Provincial and Union Bank of England* [1923] All ER 550, at 555 and 558; *Robertson v Canadian Imperial Bank of Commerce* [1990] LRC (Common) 35.

19 Lord Justice Atkin in *Tournier v National Provincial and Union Bank of England*, supra, 560–1.

20 It is expected to come into effect in December 2005.

Milestone 3: The Abacha funds recovery

The full extent to which Abacha helped himself to Nigerian public resources (1993–1998) has probably not been quantified. It is estimated to be in the region of USD 4 billion. After an extended forensic investigation and asset-tracing endeavour, which was driven by President Obasanjo, about USD 600 million has been handed over to Nigeria by Switzerland alone. Members of the Abacha family and his business associates had more than 140 banking accounts in that country!

In addition, GBP 200 million has been retrieved from banks in Britain and GBP 300 million are frozen in bank accounts in Luxembourg and Liechtenstein, bringing the tally to USD 1.1 billion.

Milestone 4: The successes of the Asset Forfeiture Unit in South Africa

Since its establishment in 1999, the Asset Forfeiture Unit has been visible in pursuing proceeds of organised crime in South Africa. Relying on methods developed in the US, the Asset Forfeiture Unit has scored notable successes against notorious drug dealers, commercial fraudsters, smugglers, armed robbers and motor vehicle thieves. The unit relies on provisions of the Prevention of Organised Crime Act (1998) that permit the forfeiture of property tainted by criminal activity through civil action. Such action enables the state to confiscate suspected criminals' assets purely through a civil action against the property without the need to obtain a criminal conviction against its beneficial holders.[21]

Such of the proceeds of crime as are not passed on to victims are invested in law enforcement, through the Criminal Assets Recovery Fund.

In the corruption case involving Schabir Shaik, financial advisor to South Africa's President Jacob Zuma who was Deputy President at the time of the criminal case in 2005, the Asset Forfeiture Unit relied on a conviction to base the application for confiscation. In many other cases, the unit has taken proceedings which either run parallel to the criminal case or are independent of it. In February 2006, the unit secured a court order to freeze a residential property belonging to a former Nigerian state governor, Diepreye Alamieyeseigha (Mr Alamieyeseigha), on the Cape Town waterfront. Mr Alamieyeseigha was charged with 39 counts of money laundering in Nigeria. An application to freeze, first the rental income from the apartment and later his interest in the apartments themselves, was successful.

The Asset Forfeiture Unit has also recovered property from recently convicted fugitive Billie Rautenbach (Mr Rautenbach), the former owner of Wheels of Africa and Hyundai Motor distributors. As a result, Mr Rautenbach paid a fine of R 40 million (USD 5 million).

VI. Conclusion

In evaluating recent achievements in recovering the proceeds of crime, it would be useful to bear in mind the dichotomies between predatory crime and market-based crime, as well as between proceeds of crime that do not leave the region and proceeds

21 See note by Martin Schönteich in ISS Crime Index, 2000, Vol. 4, accessible at www.iss.co.za/Pubs/CRIMEINDEX/00VOL4NO3/Assetforfeiture.html.

that are transferred abroad. The challenges crystallised in Gully-Hart's paper pertain mainly to proceeds transferred abroad.

As a general observation, it appears that civil forfeiture is still in limited use in most of the sub-region. Some countries regard civil asset forfeiture with disdain, even suspicion, on account of a historical association with practices that were repugnant. Legislative provisions that permit greater leeway to law enforcement in detecting the proceeds of crime, mainly corruption, have been adopted in several countries, notably Botswana, South Africa, Tanzania and Swaziland. They do not, however, seem to be utilised regularly. In addition, a large regulatory loophole exists in certain parts of the sub-region, particularly Angola, the Democratic Republic of the Congo, Malawi and Zimbabwe. Penetrability of offshore investment centres in terms of access to information is still a cause for concern.

A common thread that links the factors in the assessment by Levi is the inadequacy of information to support victims and claimants in identifying and pursuing proceeds of crime. It appears that ameliorating the current unsatisfactory situation must involve changes not just to the criminal justice systems, but also to regimes that regulate access to information. In addition, there is more that should be done to make up-to-date information on economic crime and patterns of movement of the proceeds of such crime available.

ALAN BACARESE*

The role of intelligence in the investigation and the tracing of stolen assets in complex economic crime and corruption cases

'Men may be without restraints upon their liberty; they may pass to and fro at pleasure: but if their steps are tracked by spies and informers, their words noted down for crimination, their associates watched as conspirators - who shall say that they are free?'[1]

I. Introduction

The use of intelligence-based techniques to investigate complex criminal investigations is now becoming increasingly the international norm. Although intelligence provides a platform for many different aspects of an investigation, it has a particularly prominent role to play in the tracing of the proceeds of serious economic crime and corruption. In the case of complex economic crime and corruption investigations where there is often a myriad of personalities and different complex financial vehicles often used in overseas jurisdictions, the use of differing forms of intelligence has become a 'must have' tool, and proved critically important to initial research into allegations of corruption but also subsequently in substantive investigations. As a mechanism to pursue stolen assets, it has few competitors.

Although undoubtedly in existence as a tool prior to the terrorist attacks in the United States (US) in 2001, the use of intelligence has increasingly been refined to a new level since that date. However, the challenges as to how to deal with intelligence and disseminate it in a manner that is secure, legitimate and effective remain significant. This chapter attempts to define what intelligence is, how it is received, how it is put to effective use by the law enforcement community. The chapter will also consider how intelligence can be improved, given the overwhelming challenges that face the law enforcement community in the onslaught of serious economic crimes and corruption and the manner in which the financial trails of moving the proceeds of criminal activity are becoming increasingly complex to follow in a globalised financial world.

II. Definition of intelligence

There is great deal of conjecture on what precisely intelligence is, and as a result, raw information is often perceived, incorrectly, as intelligence. Information received from

* Alan Bacarese, a United Kingdom Crown Prosecutor seconded by the Crown Prosecution Services to the Basel Institute on Governance's newly-created International Centre for Asset Recovery (ICAR), based in Basel, Switzerland, provides legal and practical expertise in the growing field of international asset recovery.

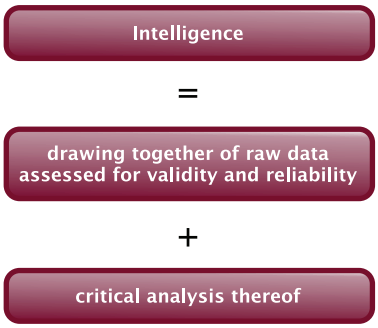
1 T. May, Constitutional History of England (1863), 275.

disparate sources such as informants, telephone complaint lines or banking records is just raw information with little context and often, therefore, no intrinsic value. It is the drawing together of such raw data assessed for validity and reliability and its analytical processing that provides the all important intelligence product for the law enforcement agencies. Analysis lies at the heart of the intelligence process.

To assist in the definition, the International Association of Law Enforcement Intelligence Analysts (IALEIA) states that intelligence is an analytic process:

> '…deriving meaning from fact. It is taking information collected in the course of an investigation, or from internal or external files, and arriving at something more than was evident before. This could be leads in a case, a more accurate view of a crime problem, a forecast of future crime levels, a hypothesis of who may have committed a crime or a strategy to prevent crime.'[2]

Intelligence, in the context of the law enforcement community the world over, is therefore essentially about the flow of information and how that information is evaluated, analysed and disseminated to law enforcement agencies. As the product of an analytical process that evaluates information collected or provided from potentially many diverse sources, one of the main challenges is how to package the product in a manner that provides meaningful and value added direction to law enforcement agencies about complex criminal activity, and either adds to a greater understanding of the way in which criminals and their enterprises work or how they are continuing to commit criminal activity. In the context of serious economic crimes and corruption, and the tracing of assets derived from such crime, intelligence is the key to understanding how criminal proceeds flow and, ideally, where the proceeds are.



It is evident, therefore, that the intelligence received need not always be just hard information for use in targeting the suspects in the investigation, or tracing their assets, but may also be used in a more tactical manner to develop assessments on threats and strategies to deal with such threats, allocate resources and provide overall a more effective response to those threats.

It is also important to recognise the much broader role that intelligence plays in the context of law enforcement, as the investigative phase of any investigation is much more focused in the sense of seeking information and evidence for possible use in subsequent criminal proceedings. This process naturally attracts more circumspection as the rules of evidence, and how evidence is acquired, apply. However, this is not to say that the pursuit of intelligence is without any checks and balances – or rather it should not be! But the broader role of intelligence does permit the law enforcement

2 International Association of Law Enforcement Intelligence Analysts. (undated). Successful Law Enforcement Using Analytic Methods - Internet-published document.

agencies more time and more latitude to develop the intelligence to a point where they have enough credible and substantiated intelligence to take it to the next level, namely a full blown investigation.

The requirement for proper checks and balances within a system of gathering information about individuals should be tight. There should be proper structures in place to ensure that the information is kept secure and that when the information is shared with either other domestic agencies, or, in particular, other international agencies that this is done in a structured and safe environment. The sharing of such information will be much more fluid and therefore effective if all parties agree to adhere to guidelines and international standards. This point is considered in more detail below when we consider the use of financial intelligence and the role of financial intelligence units in the tracing of assets.

But from a process perspective, what is meant by intelligence sharing? How can the appropriate law enforcement agencies be integrated into the intelligence sharing function? On a more fundamental level, what information can be collected and what information can be kept in files? How long may it be kept in files? To ensure an effective law enforcement response, these critical questions must be answered.

III. The processing of information into intelligence

All assessments of information provided should aim to describe the reliability of the source and of the information provided, to distinguish between reported facts and comment and to provide as much detail as possible. To do this, the analysts working on such processing must use their skill to consider the relevance of the information which will largely depend upon the provenance and reliability of the source of information and the information itself. In many intelligence agencies, there will be some mechanism, or a process of reporting, to assist in this evaluation

The United Kingdom's (UK) Serious Organised Crime Agency (SOCA), which undertakes many intelligence assessments including the UK's financial intelligence assessments, asks six standard questions, which try to avoid the dangers of a list that might be too long or too short, when attempting to establish the value of information received: Who?, What?, Where?, When?, How?, and Why?[3] The following pointers provide some useful indicators on what is being sought under each heading.

Who?

- Full name, plus any other identifying personal particulars, such as date of birth, current address, aliases, nicknames
- Criminal records reference number, or other adverse records, including previous intelligence traces
- Nationality, ethnicity, immigration status, language(s) and dialect(s)
- Family members, and the extent of their involvement

What?

- Main criminal activities, other criminal activities
- Scale and frequency of criminal activities

3 Taken from the national intelligence requirement for serious organised crime 2008-9 SOCA.

- Nature of involvement, role
- Associates and contacts, including the nature of the relationships
- 'Legitimate' business activities

Where?

- Main locations of criminal activities, plus reach ('turf') or spread
- Use of vehicles and other means of transport, including driving licence details and vehicle registration numbers
- Travel details, including passport details, routes

When?

- Actual dates, times
- Periods (from/to)

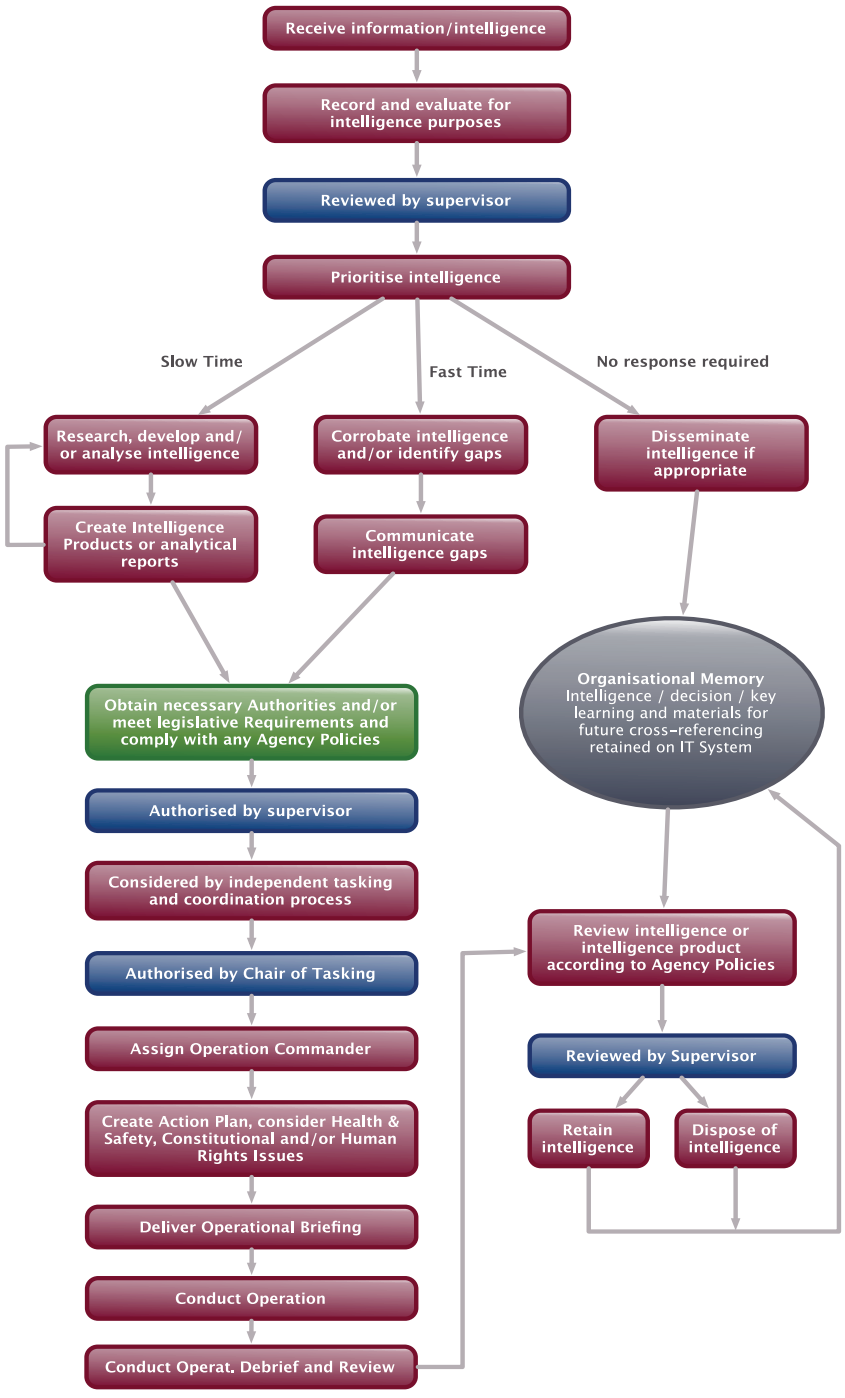
How?

- Criminal methods (how the business is organised and conducted)
- Means of communication, including telephone numbers, Internet use, use of coded language
- Assets employed (e.g., premises, vehicles, personnel)

Why?

- Rationale for particular actions and choices
- Motivation
- Attitudes (e.g., towards risk, criminal opportunities)
- Lifestyle (use of criminal profits to fund property purchases, vehicles, 'nest eggs', family support, entertainment, holidays, etc.).

The flow chart below provides a brief overview of a generic intelligence model and details how information is received into the intelligence system and how it is processed and disseminated depending upon its nature and also whether there is a need to task the intelligence for action purposes.



IV. Different types of Intelligence

The amount of information and its sources that are available to law enforcement agencies who have developed an intelligence strategy, or are about to, is extensive,

although it will vary in different countries. The types of information available that might be then cultivated for intelligence purposes could include the following;

- The statements or depositions of victims and witnesses
- Information from hotlines or from the public
- Informants
- Surveillance and other types of covert operations
- CCTV and other public surveillance systems
- Commercial agencies, e.g., banks and credit card agencies
- Police information technology (IT) systems such as law enforcement national computers that may retain information on previous convictions and traffic enforcement databases, for example
- Other law enforcement agencies
- Internet and other open sources techniques
- The media

There are many different types of intelligence that we could address in greater detail. We have selected three of the most important in the context of the tracing of the proceeds of serious economic crimes and corruption, namely:

- Financial intelligence
- Human intelligence
- Open source intelligence

1. Financial intelligence

Pursuing criminals' finances is now accepted as one of the most important ways in which law enforcement agencies can acquire intelligence and establish evidence against criminal activity. It is now firmly established that criminal monies are invested in further criminal activity, saved or invested in assets, some is used to pay off costs of operations or to secure the services of other corrupt individuals and certainly much of it is used to fund criminal lifestyles. Therefore, it stands to reason that in any investigation into offences that have an acquisitive nature, such as corruption, or that involve the movements of money, one of the most important sources of intelligence for law enforcement agencies the world over is financial intelligence.

The increase in the value of financial intelligence has been dramatic over the last decade or so. This is particularly so when one considers the growth of financial intelligence units (FIUs) across the world. In 1995, the Egmont Group of Financial Intelligence Units was created, an informal international gathering of FIUs. As of September 2009, the Egmont Group consists of 116 FIUs from across the globe. The FIUs are national centres to collect information on suspicious or unusual financial activity from the financial industry and other entities or professions required to report transactions suspicious of being money laundering or terrorism financing. About one third of the Egmont Group members are not law enforcement agencies; their mission is to process and analyse the information received. If sufficient evidence of unlawful

activity is found, the matter is passed to those agencies responsible for investigation or prosecution of such matters.[4]

FIUs, generally speaking, receive, analyse, and disclose information by financial institutions, or other entities such as lawyers and accountants that are under an obligation to report, to competent authorities of suspicious or unusual financial transactions. Critically important is the ability of many of the FIUs, under certain provisions, to be able to exchange information with foreign counterpart FIUs. One of the main goals of the Egmont Group is to create a global network by promoting international cooperation between FIUs. It is this exchange of important financial information between the FIUs in an informal process (which by definition speeds up the system of information exchange dramatically) that contributes so much to the intelligence gathering and dissemination process.

The nature of the information gathered by the FIUs is extremely varied. Although much of the information that is gathered is the product of legislative obligations to submit suspicious activity reports to FIUs, intelligence can also be proactively sought by the FIUs to build up profiles of individuals and money laundering techniques, for example.

By way of an example, we highlight the types of reports that are regularly submitted to the US FIU, the Financial Crimes Enforcement Network (FinCEN),[5] and the thresholds that are applied.

4 Egmont Press Release, Doha 28 May 2009 - Expanded Egmont Group focuses on the vital role of FIU's in Strengthening International Cooperation and Exchange of Information in the fight against Money Laundering and Terrorist Financing.

5 FinCEN is the US FIU and stands for the Financial Crimes Enforcement Network which was created in 1990 to provide a government-wide multi-source financial intelligence and analysis network. The organisation's operation was broadened in 1994 to include regulatory responsibilities for administering the Bank Secrecy Act, one of the nation's most potent weapons for preventing corruption of the US financial system. The Bank Secrecy Act (BSA), enacted in 1970, authorises the Secretary of the Treasury to require certain records or reports where they have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, or in the conduct of intelligence or counter-intelligence activities, including analysis, to protect against international terrorism.

Representative Reports required from US financial institutions

Report and definition	Authority	Receiving Agency
Currency Transaction Report (CTR). Cash transactions in excess of USD 10,000 during the same business day. The amount over USD 10,000 can be either from one transaction or a combination of cash transactions.	Bank Secrecy Act[6]	Internal Revenue Service
Negotiable Instrument Log (NIL). Cash purchases of negotiable instruments (e.g., money orders, cashiers checks, travellers cheques) totalling from USD 3,000 to USD 10,000, inclusive.	Bank Secrecy Act	Internal Revenue Service
Suspicious Activity Report (SAR). Any cash transaction where the customer seems to be trying to avoid BSA reporting requirements (e.g., CTR, NIL). A SAR must also be filed if the customer's actions indicate that s/he is laundering money or otherwise violating federal criminal law. The customer must not know that a SAR is being filed.	Bank Secrecy Act	Financial Crimes Enforcement Network

Just to assist the banking institutions and other regulated entities, FinCEN also advises that the following may trigger the need for the reporting of a SAR:

- Any kind of insider abuse of a financial institution, involving any amount
- Federal crimes against, or involving transactions conducted through, a financial institution that the financial institution detects and that involve at least USD 5,000 if a suspect can be identified, or at least USD 25,000 regardless of whether a suspect can be identified
- Transactions of, at least, USD 5,000 that the institution knows, suspects or has reason to suspect involve funds from illegal activities or are structured to attempt to hide those funds
- Transactions of, at least, USD 5,000 that the institution knows, suspects or has reason to suspect are designed to evade any regulations promulgated under the BSA or
- Transactions of at least USD 5,000 that the institution knows, suspects or has reason to suspect have no business or apparent lawful purpose or are not the sort in which the particular customer would normally be expected to engage and for which the institution knows of no reasonable explanation after due investigation.

This level of guidance means that in the fiscal year ended 1 October 2008, FinCEN received slightly more than 18 million BSA reports[7], marginally up from the figure of

6 The Bank Secrecy Act is the popular name for the federal financial reporting, recordkeeping and anti-money laundering requirements and prohibitions codified at 12 U.S.C. 1829b, 12 U.S.C. 1951-1959, and 31 U.S.C. 5311-5332. FinCEN regulations implementing the Bank Secrecy Act can be found at 31 CFR Part 103.

17.9 million in the fiscal year 2007. With this level of reports on financial transactions, it is critically important to FIUs to receive as much of that material in electronic form so that it can be processed much quicker using special databases.

As the law enforcement agencies of the world begin to mainstream the use of financial investigations, they are being deployed increasingly against groups of organised criminals and corrupt officials who, for a long time, have been beyond the law. Financial intelligence is now able to assess the vulnerability of such people to a financial investigation and also expose them to asset recovery procedures. The international nature of global finance, make those previously seen as 'untouchable' vulnerable to attacks on their assets.

In the UK, where the FIU is now housed in the SOCA, these financial intelligence tools are increasingly being utilised in investigations against the type of criminals described above. For example, in 2007, the leader of a dangerous and violent criminal gang operating across London was identified by law enforcement agencies. Although he and the gang posed a serious and sophisticated threat to the public, use of 'traditional' policing methods had been unable to disrupt their criminal activities – several attempts by specialist units to prosecute members of the gang had failed. A financial investigation was undertaken to identify the gang leader's associates, and traced properties he had purchased using false information. A restraint order was served on the gang leader, preventing him from moving his assets. He was successfully prosecuted for money laundering and his assets were confiscated. Three other members of the group were prosecuted for attempted murder and drug trafficking. All these prosecutions would have failed without the evidence uncovered by the financial investigation.[8]

2. Human Intelligence

The law enforcement community has always dealt with persons coming forward for a multitude of reasons to complain about the conduct of others. It might be that the information comes forward as part of community engagement or, in the case of serious economic offences and corruption, the individual who comes forward may well be a disgruntled former employee, a whistleblower, a company representative who has been cheated out of a procurement deal by large-scale bribery or even a former co-conspirator with an axe to grind. In either case, the law enforcement agencies have a duty to protect the confidentiality of the individual, and their personal and professional risk but also to weigh up how they are to deal with potentially critical information, which could be developed into important intelligence, but which might be tainted.

In terms of evaluation of the information provided, the intelligence analysts will have to pay considerable caution to the reasons for the individual wishing to pass on information, what possible motives might exist, whether those motives might be malicious, and therefore misleading, with the potential to compromise the intelligence and subsequently the investigation, and whether any sort of inducement is sought for the information. The intelligence analysts will have to work hard to corroborate the information provided in many circumstances.

On a human level, the circumstances of how the information came to be offered will have to be evaluated carefully to ensure that the individual is not at personal risk. For

7 This figure includes all BSA reports which will include SARs – 600,000 to 700,000 – but will also include larger amounts of Currency Transaction Reports, cross border reports (CMIRs) and Foreign Bank Account Reports (FBARs).

8 Extending our Reach: A Comprehensive Approach to Tackling Serious Organised Crime, Cabinet Office and Home Office, July 2009.

example, they may be part of a corrupt network and still exposed to the potential for some personal harm or the individual may also be still in the employment of the person who is the subject of the information. However, despite the potential for risk, human intelligence sources remain one of the key operational tools for law enforcement agencies, particularly in circumstances where there is a real lack of information about the corrupt network in question, to which are notoriously difficult to gain access, and the individual is prepared to continue to provide further information. The human rights or constitutional issues at stake in such a process are considerable. One of the first considerations is the extent to which non-law enforcement personnel can be used to undertake the role of acquiring evidence on behalf of law enforcement, given the risk to the individual but also to the operation itself. There is additionally a question as to how far the individual can also report on activities of the suspects and what documents, for example, he might be permitted to seize within the letter of the law. Furthermore, there is also the risk that the individual goes too far and commits criminal offences him/herself or incites the commission of an offence, providing the suspects with the opportunity to argue some form of abuse of process or entrapment arguments in subsequent hearings.

3 Open source

One area of intelligence gathering that has seen a real growth in recent years has been the use of open source techniques. Indeed, the technique is now leading to access to so much high quality and insightful evidence intelligence that it led to the 9/11 Commission recommending that a new Open Source Agency be added to the US intelligence structure.[9]

Open source intelligence is a form of intelligence gathering that involves finding, selecting and acquiring information from publicly available sources, such overt, publicly available sources (as opposed to covert or classified sources) and analysing such information to produce credible intelligence. Open source is distinguished from research in that it applies the process of intelligence to turning hard data and information into intelligence to support strategic and operational decisions.

Understandably the Internet provides a great deal of information for the analysts and simple checks can be made on a name or address which may reveal details which can be of use to intelligence development. The effective use of the Internet in this way, however, is a specialist area of work, and secure methods of searching must be employed so as not to compromise operations.

Open source information is wide-ranging and includes, amongst other materials, the following:

- All types of media
- Directories
- Databases of people, places, and events
- Social networking sites and web-based communities such as chat rooms
- Government reports and documents
- Scientific research and reports
- Statistical databases

9 National Commission on Terrorist Attacks Upon the United States. (2004). The 9/11 Commission Report. Washington, DC: U.S. Government Printing Office, 413.

- Publicly available databases
- Commercial vendors of information
- Websites that are open to the general public even if there is an access fee or a registration requirement
- Search engines of Internet site contents

The information obtained from open sources tends to fall into two categories, namely one involving information about individuals, and, secondly, involving aggregate information. The aggregate information available is extensive which is where the skills of a qualified analyst come into play as it is a real challenge to assess what is reliable and what is relevant for the purposes of constructing intelligence. Consider some of the new databases, often commercially available, that are emerging which are able to provide enormous detailed analysis of current trends, companies and individuals. It is no surprise therefore that law enforcement agencies are now increasingly using these methods.

However, agencies must remember that when the information that is being gathered via open source relates to individuals and is being retained as intelligence, there is a strong possibility that human and constitutional rights may well attach to this information. As open source can lead to the mining of important and sensitive information about an individual, for example, a person's credit rating; once that information is retained and forms part of an intelligence assessment and a file, questions and processes need to be carefully considered to ensure compliance with the broader issues under human and constitutional rights.

Generally speaking, the key is not the source of the information about the individual but what is being retained and how it is being retained by a law enforcement agency. In such circumstances, law enforcement agencies may need to carefully consider what types of open source information about a person should be kept on file when that person is not actually a suspect or where the individual has only a passing relevance to a proper suspect or particular activity that is under consideration by the law enforcement agency. And what about the situation where the open source research establishes a tangential link between suspects which is neither confirmed nor able to be corroborated by intelligence? The ability to retain information about individuals on databases is too easy and therefore careful consideration must be given to this matter. The source of this information is irrelevant.

Nevertheless, open source techniques and access to news media, for example, are capable of yielding a tremendous amount of information that should be part of a law enforcement agency's 'intelligence toolkit'. It should be incorporated as part of an agency's intelligence plan.

V. Conclusion

This chapter has attempted to provide an insight into what intelligence is, its role, and some of the complications that emerge from the use of such techniques. In the context of corruption and serious economic crimes, it has attempted to provide an overview of the increasingly important significance of the use of intelligence, as opposed to mere information, in the fight against such crimes including the tracing of stolen assets or the proceeds of unlawful activities. However, despite its undisputable value, it is high level support and the recruiting of the correct staff – trained analysts, for example – that remain the key. The mandate of such intelligence units will largely depend upon the resources available, levels of skills of personnel, and what structures currently

exist. The other issue of real importance is the need to interact with other agencies. To this end, it is the design of a systematic method of collecting, assessing and prioritising information into effective intelligence that will greatly aid the process. What we now know is that the simple building of file upon file of information on individuals and areas of criminal concern does not provide any insight and leads to information that is of little value. Finally, given the complex nature of the offences under discussion in this chapter, and the real problems and difficulties of tracing the proceeds of crime as they cross international boundaries, the greatest capacity required for this work is the need for intelligence operatives to be proactive, to test new areas of research, within the legal constraints and to develop unique products that will provide a steady stream of high quality and reliable intelligence to the law enforcement agencies on a consistent basis.

TOM LASICH*

The investigative process – a practical approach

I. Introduction

The investigative process is the core activity that must form the basis for any asset recovery effort. A jurisdiction where funds have been secreted will not confiscate or repatriate the assets to the country of origin unless evidence is presented, linking them to an illegal activity. This evidence must be admissible in court proceedings. There are basically two ways in which the evidence can be collected. Law enforcement officials in the country where the illegal activity occurred can conduct an investigation using all available legal authorities. Alternatively, a private law firm can be retained to file suit in the jurisdiction where the assets are located. This chapter will focus on an investigation conducted by the government, using its broad range of law enforcement powers.

What is the goal of this investigation? This singular financial investigation will actually have multiple goals. Firstly, it will connect the asset to the corrupt or illegal activity. This will form the basis for confiscation, and can be accomplished through the collation and presentation of either direct or circumstantial evidence. Secondly, the investigation should establish sufficient evidence to prosecute the corrupt official on criminal charges of both corruption and money laundering. Thirdly, the evidence gathered will also enable the country to trace and identify assets that have been stolen or misappropriated. Therefore, the asset tracing, the money laundering investigation, the establishment of the corruption charges and the seizure of assets are all, in essence, the same investigation. This will form the cornerstone for the eventual repatriation of the stolen funds.

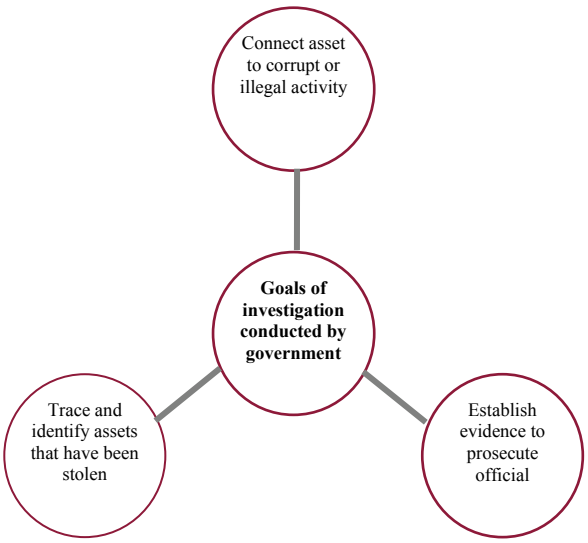


Fig. 1: The core goals of the investigative process

* Thomas D. Lasich is currently the Head of Training for the Basel Institute on Governance, International Centre for Asset Recovery (ICAR) section in Switzerland. He worked in federal law enforcement in the United States conducting financial investigations and presenting money laundering, anti-corruption and financial investigative technique training programs for 37 years.

How should the investigative process be structured? Large-scale monetary corruption cases should always have a focus on how the money was paid and who received the benefit. The financial investigative portion of the case can be conducted in a variety of ways, depending on the circumstances of the case. The major strategies that can be employed are summarised as follows:

- Specific item case, using direct evidence
- Direct proof of bribe, through audio and video provided evidence
- An indirect method of providing income, using circumstantial evidence
- Proving the true purpose of a series of concealed or fraudulent transactions, using circumstantial evidence

What sort of cases or fact patterns would require the use of one of the above methods? Let's explore some examples which illustrate when each of these financial investigative techniques could be used to assist in proving the criminal violations and tracing assets.

1. Specific item

This method would be used when specific payments of bribery or misappropriated government funds can be traced to the official's direct benefit. The evidence would directly prove the linkage between the corrupt activity and the value received by the public official.

2. Direct proof of bribe

An undercover or covert operation may be able to develop direct evidence of a bribe. On rare occasions, an informant or a representative of a private company may provide information to law enforcement that a bribe has been solicited from him by a public official. In this instance, it may be possible to set up surveillance video and audio equipment that will document the bribe transaction.

3. Indirect methods of proving illegal income

If illegal income cannot be traced directly to the corrupt official, then an indirect method of proof may be required to corroborate evidence of corrupt payments. For example, if it can be proven that the official spent money during a set period of time that was substantially in excess of his legal income, this could be used as circumstantial evidence to prove the amount of illegal income that the person received. In a corruption or money laundering case, this type of proof would be used in conjunction with other evidence that established the corrupt activity such as bid rigging or other misappropriation of funds. If the intended criminal charge was unjustified or unexplained wealth, then the indirect method of proving income may be the main evidence in the case.

There are two main methods for proving illegal income through an indirect method. These are the Net Worth method and the Source and Application of Funds method (also referred to as the Expenditures method). There is also a method called the Cash Flow Analysis but it has been used less frequently. The Net Worth method is considered to be somewhat confusing and difficult to explain at trial. The concept of the Source and Application method is relatively simple, and is the preferential indirect method of proving income in most cases. The basic theory for this method is that the

person under investigation spent far more money during a set period of time that he had legally available to him.

4. Proving concealed or fraudulent transactions using circumstantial evidence

There are some cases in which neither the specific item method nor an indirect method such as the Source and Application of Funds would be appropriate. The case may have no direct linkage between the corrupt activity and the acquired wealth of the public official. Additionally, the increase in wealth attributed to the official may appear to have been legitimate. In cases such as this, the investigation may have to analyse the specific transactions that resulted in the official's increase in wealth. It may be necessary to trace the transactions through a series of prior property owners to arrive at the true nature of the operations.

One of the best ways to explain the investigative process is by way of example. The brief simulated case below takes the reader through a typical corruption investigation – if one can call any case typical!

II. The allegation

1. Suspicious Transaction Report

The government of country A has just received an official letter from the Swiss government advising that one of their banks has received suspicious electronic funds transfers in excess of USD 8 million to an account held by the son of country A's Deputy Minister of Internal Development.[1] The account was opened 14 months ago. Under the Swiss bank's money laundering controls with regard to Politically Exposed Persons (PEP), the transaction had been flagged as suspicious and a temporary freeze put on the funds. The letter stated that no additional information concerning this account can be disclosed at this time. However, upon receipt of an official mutual legal assistance (MLA) request, the account details may be provided following disclosure proceedings. The letter indicated that the request should include the nature of any criminal investigation being conducted in country A, the potential criminal violations, a summary of the investigative efforts and all additional MLA requirements. There have been rumours for many years that the Deputy Minister lives beyond his means but no investigation has ever been undertaken.

2. Investigation planning and strategy

Is the information from the Swiss government important? What should be done first? Can a MLA request immediately be filed with the Swiss government to seize the bank account? Should the Deputy Minister be placed under investigation? These are all questions that need to be answered very quickly. The facts of each case will vary, and the investigative decisions and actions will depend on the individual circumstances. The legal system, criminal procedures code and investigative practices for each country will, to some degree, dictate the process to follow. However, to the extent possible, the decisions, based on the facts stated above, should be made quickly and coordinated through a multi-agency approach.

1 Based on Article 67a of the Federal Act on International Criminal Assistance, the Swiss authorities can spontaneously transmit information to a foreign state when it determines that this transmittal can permit the opening of a criminal proceeding.

The first question that some may ask is 'Can we seize the money and have it returned to our country?' This would be a mistake to attempt to seize the money at this stage. One has no information that the money was illegally obtained. If a request is sent to the Swiss government to seize the funds, it would most likely be rejected because there has been no investigation and, in fact, there are not even any allegations – only rumours – that the Deputy Minister is living beyond his means. This request would only result in the loss of valuable time.

The letter from the Swiss government indicated that a temporary freeze had been placed on the account. The first step would be to immediately contact the sender of the letter and ask some questions to clarify a few issues. What are the issues and who should make the call? The most important issue is how long will the temporary freeze be held on the account. The second key question would be: Has the Swiss government opened an official money laundering investigation? Once one knows how long the funds will remain frozen and whether extensions are possible, then one can more accurately plan one's investigative steps and strategy. Knowing if the Swiss government has opened an official investigation will immediately tell the investigator if he or she has a partner in this potential investigation. This will lead to a more efficient sharing of information and evidence in the months to come.

Who should make this initial call? The answer will depend on who received the letter – the central authority for MLA, the Ministry of Justice, the Foreign Affairs Office or some other agency. The executive structure of the government will certainly dictate the answer to this question. The important point is that a decision should be made to determine the appropriate person very quickly. Time is of the essence. These funds may only be frozen for five days or possibly for 90 days but the investigator needs this information so a call must be made. In this instance, one would place the phone call and speak with the prosecutor of the Confederation or of a Canton (a Swiss administrative subdivision of the country) who sent the letter. The investigator is informed that the freeze is for 60 days; eight days have already passed; the freeze can be extended for another 60 days if additional evidence is provided through proper legal channels. The investigator also learns that the prosecutor has opened an official money laundering investigation. The prosecutor advises the investigator that he cannot provide any additional details of the account until he receives an official MLA request which contains information to the effect that country A has taken investigative steps. He further states that the request must contain new information or evidence that has been gathered in country A. Simply returning the same information that he has provided in his letter in the first instance will not suffice.

3. Pre-investigative steps

A preliminary investigation should now be initiated by the lead agency – possibly the anti-corruption unit or some other appropriate agency depending on the structure of the government. This lead agency should quickly gather all available information during this pre-investigative stage. This will generally include information that can be obtained without making overt investigative inquires that would alert the public. All national law enforcement and commercial databases would be checked; inquiries would be made to other government and investigative agencies; the financial intelligence unit would be queried for suspicious transactions; and limited surveillance may be conducted to determine additional property that the Deputy Minister may own. The results of these pre-investigative inquiries disclosed the following:

- The Deputy Minister's government income is approximately USD 120,000 per year.
- His required wealth disclosure statement indicates that he maintains a domestic bank account in the capital city of your country.
- His wife is unemployed and drives a Mercedes valued at USD 80,000.

- He resides in a house that was purchased two years ago for USD 850,000 that currently has a mortgage of USD 300,000.
- He has two sons who both attend universities in the United Kingdom (UK).
- His office has awarded 23 sole source contracts in the last three years for infrastructure development projects totally in excess of USD 195 million.

III. An authorized investigation

Based on these facts, the Director of the lead agency initiates a full investigation.

1. Communication with foreign counterparts

The pre-investigation stage took 40 days to complete. Now that a full investigation has been authorised, what steps should be immediately taken? What is the status of the frozen funds in Switzerland? In 12 days' time, the freeze will be lifted and the funds can be moved around the world in a matter of minutes through electronic funds transfers. The preparation of a formal MLA request, processing it through the central authority, transmitting it to the central authority of Switzerland and having it forwarded to the prosecutor will take at least one month. What options does the investigator have to prevent the freeze from being lifted and the funds disappearing? The answer is simple. It is again based on communication and developing a relationship with your foreign counterparts. The prosecutor in Switzerland had previously advised that the freeze could be extended for an additional 60 days, based on new evidence. A telephone call should be placed to the prosecutor, asking him for advice on the best way forward. The investigator then learns that the prosecutor will accept a letter stating that an investigation is underway in country A, additional information has been obtained on the Deputy Minister and that the investigator is in the process of filing a formal MLA request. He advises that once this letter is received, he can extend the freeze on the account. He also states that the freeze can be continued as more evidence is developed. This letter must now be prepared and immediately sent to the Swiss prosecutor to protect the assets from being moved.

2. Compilation of MLA request

At the same time, a formal MLA request must be prepared and submitted to the Swiss government. What format should be used for this request? How should it be transmitted? What actions should be requested?

Format of request

The answer to the first question is relatively easy. There are 192 member countries of the United Nations and a few other countries with limited international recognition. So how would one know what MLA format each country needs? Again, communication is the key to fast and efficient international cooperation. Prior to drafting the MLA request, place a call to the central authority of the requested country and ask for their MLA template, explain the request, seek advice and finally inquire if an advance e-mail copy of the MLA request can be sent to them for their review. Most jurisdictions will be pleased to assist an investigator with the formatting, substantive requirements and general guidance. Without taking this very simple step, one risks losing months of valuable time if one's MLA request is rejected and returned for corrections.

Transmittal of request

The second question, namely, how should it be transmitted, is critical. The courts in many jurisdictions will not allow evidence obtained from a foreign country to be admitted unless it is obtained through the proper channels. Each country should have a central authority. This is the designated government body that is authorised to send and receive MLA requests. For example, the United Nations Convention against Corruption (UNCAC) (Article 46 paragraph 13) requires that

> 'Each State Party shall designate a central authority that shall have the responsibility and power to receive requests for mutual legal assistance and either to execute them or to transmit them to the competent authorities for execution.'

The Article continues to explain that

> 'The Secretary-General of the United Nations shall be notified of the central authority designated for this purpose at the time each State Party deposits its instrument of ratification, acceptance or approval of or accession to this Convention. Requests for mutual legal assistance and any communication related thereto shall be transmitted to the central authorities designated by the States Parties.'

Nature of requested actions

The third question, namely, what actions should be requested, is also of great importance. The investigator knows that there is a bank account in Switzerland that is held in the name of the son; there are incoming electronic funds transfers into the account in excess of USD eight million; the Deputy Minister has two sons, both of whom are students; and the account is currently frozen. One may want to confiscate the funds in the account and have them immediately repatriated to your country but it is probably premature to request these actions. There are two main activities that one should request. Firstly, based on the limited evidence that has been gathered through one's pre-investigation, one would like to have the freeze order extended on the account while the full-scale investigation progresses. Secondly, the records of the bank account should be requested for a specific period of time – in this case, from the opening of the account 14 months ago to the present. What records should be requested? This is a critical question. One's request should be very specific and also provide for follow-up inquires if appropriate. When requesting the specific documentation, the investigator may want to consider using language such as 'including but not limited to'. This gives the receiver of the request a definite list of required documents but allows them to provide additional related documents of which you may not have been aware. In this case, one will want to request items such as the following:

- The account opening documentation (know your customer information) and any due diligence that may have been conducted as a result of the PEP rules that are in place
- Information from the bank explaining why the transactions were considered to be suspicious
- All bank account periodic statements
- The details of all items credited to the account. This would include the specifics of all electronic funds transfers, showing the original bank and account name and number. Knowing the specific source of each deposit is extremely critical
- The details of all debit items. Again, this would include the ultimate beneficiary of any electronic funds transfers
- All correspondence files. This is often where the best evidence is obtained, particularly if an account manager is assigned to the client. Small notes or formal documentation that may have been placed in the file by the account manager could disclose personal relationships, the purpose of transactions or false statements concerning the person's background or business. These false statements can later be used as evidence to proof the concealed purpose of the account activities
- Loan Files. This may be the source of numerous additional leads. If the person obtained a loan form the bank, there will probably be a loan application that lists the source of income, assets, personal references and other loans
- Credit card statements, application and payment history. This information often needs to be requested specifically. The bank may not routinely provide credit card information when bank records are requested. The payment history on credit cards may be of particular interest. Payments on the account may originate from cash, another account or a seemingly unrelated company

The MLA request should also ask that any leads to other accounts, persons or entities within the country's jurisdiction be followed. Communication is again the key to this type of extended request. Discussions with the central authority or prosecutor prior to filing the MLA request will provide the investigator with information relating to how far he or she can expand the request. It will also strengthen one's relationship with the authorities in the foreign jurisdiction, and provide the basis for future collaboration on additional investigative action. For example, the bank information may lead to large payments being made to a person in the same country. If the MLA request covered the possibility of following leads, then an interview may be conducted with the recipient of the funds, and one could be closely involved either through the submission of a detailed list of questions or even participation in the interview if so invited by the requested country.

Regarding the requested bank records, in most cases, the investigator will not know the volume of records contained in the account until the bank researches its files. It is usually advisable to request all possible records that may be pertinent to the case but to control the delivery of these records to the investigator as he or she assesses their relevance. For example, if the account turns out to be in respect of an active business, it may contain hundreds or thousands of records for each month, many of which may not be of interest to your investigation. If possible, start by asking the bank to provide one with only the bank statements and significant transactions such as the large electronic transfers. The bank will still be under *subpoena* or a compulsion order to

supply all records but they will only be asked to research the records as one determines the need. This will allow the investigator to quickly study the summary records (bank statements) and make an investigative decision on what records he or she would like to review next. If one asks to receive all records at once, one may wait months for the bank to gather these records and then find out that one is in possession of thousands of documents, many of which have little value.

3. Prioritisation of leads

With the guidance of the central authority in Switzerland, the investigator has now prepared and filed a complete and accurate MLA request. What is the next investigative step that should be taken? There are a number of leads that can be followed, based on the information that was discovered during the pre-investigation stage. It would be advisable to prioritise this information and select which leads may result in the development of the most significant evidence in a timely manner.

Personal residence

How shall the investigator now proceed? The personal residence is a very interesting situation because it was purchased just two years ago for USD 850,000 and the current loan balance is only USD 300,000. Therefore, USD 550,000 has been paid toward the purchase price of the house, either through large payments in the past two years or as a very large initial payment at the time of purchase. The detailed financial information relating to the purchase may be fairly easy to obtain because the house was purchased through a licensed Notary Public and the loan (mortgage) was obtained at a major bank. This bank may maintain detailed records of the transaction since they financed a significant amount and should have conducted due diligence which may have included the source of the initial payment. The Notary Public may also have records of the complete transaction. In some countries, it is customary to use 'title companies' or 'closing agents' that act as an escrow agent or middleman to facilitate the purchase of the property between the buyer and seller. These entities also maintain complete records of all money flows between the buyers, sellers, taxing authorities and financial institutions. The seller of the property should also be interviewed to obtain the complete details of the transaction, including the method of payment for the house.

Cash flow analysis

The Deputy Minister maintains a bank account at a domestic financial institution. The records of this account should be requested very early in the investigation because it may require a significant amount of time for the bank to research the records. The same type of records should be requested for this account as was indicated for the Swiss account above. If the government salary of the Deputy Minister has been deposited into this domestic account, it will be important to perform a complete analysis to establish how his legitimate salary has been spent. A cash flow analysis relating to any cash withdrawals or deposits should also be prepared. Once these financial flows have been analysed, it will create a complete picture of the distribution of his legal funds and show how much cash was available for purchases. This may be very significant if expenditures are later identified from unknown or illegal funds. Large cash payments or purchases from unknown sources may be an important piece of evidence at trial.

Corruption cases are often difficult to prove through direct evidence because the perpetrators are skilled and devious schemers who may utilise the services of lawyers and accountants to disguise the trail of the funds. Painting the complete financial picture of the corrupt official and isolating his legal income to more clearly identify expenditures from unknown sources can be important facts when presented at trial.

This type of circumstantial evidence will, of course, have to be combined with other evidence – pieces of the puzzle – to demonstrate that the money flows from unknown sources came from illegal or corrupt activities. The Organisation for Economic Co-operation and Development (OECD) has stated

> 'Proving the requisite intention is not always an easy task since direct evidence (e.g., a confession) is often unavailable. Indeed, bribery and trading in influence offences can be difficult to detect and prove due to their covert nature, and because both parties to the transaction do not want the offence exposed. Therefore, the offender's mental state may have to be inferred from objective factual circumstances.'[2]

University education

Preliminary information in the case relating to the Deputy Minister indicated that he has two sons attending universities in the UK. Further inquires disclose that the oldest son attends the London School of Economics (LSE) and the younger son is a student at Oxford University. Is there further information that the investigator would want to pursue regarding the education of these boys? What investigative action would be most efficient and beneficial? There is a very good chance that the Deputy Minister is not able to afford the tuition, living expenses and travel relating to his sons' education. The boys may be receiving scholarships and attending the universities at no cost. There is only one way to determine the true facts. The universities must be contacted, the expenditures documented and the source of payments identified.

What is the best way to pursue this investigative inquiry at the universities? An MLA request can certainly be prepared and submitted to the central authority in the UK. This process should again begin with communication by way of a telephone call to an appropriate official in the UK. The same steps as described above with the Swiss MLA request should be followed. A telephone call to the central authority asking advice on the best way forward should be the first step. However, in this situation the investigator may want to explore other options during his or her call. It may be possible that the police, the money laundering section or the asset forfeiture unit have the ability to request the desired information from the universities on an informal basis. If they do not have this ability, one has wasted approximately two minutes asking the question. But, if the answer is that they do have this ability, then one may possibly have saved four months of valuable investigative time.

How could the investigator have saved this amount of time? Let's explore two different possibilities. In the first scenario, the police obtain the information informally from the university as a result of their many years of working together. The payment records indicate that the tuition was paid directly from the Deputy Minister's domestic bank account in your country. This will save one the time and effort of filing an MLA request with the UK because one has already traced the payments to the domestic account to which one has access. In the second scenario, the payment information obtained informally indicates that the tuition was paid by a subsidiary company of a corporation that was awarded a USD 35 million contract through the Deputy Minister's office. The subsidiary company is located in a third jurisdiction. How has the investigator saved a significant amount of time? One can now file an MLA request with the UK to obtain this evidence through a formal process to assure its admissibility as evidence at trial. Simultaneously, an MLA request can be submitted to the third jurisdiction where the subsidiary company is located. Instead of waiting possibly four months for the return of the MLA request to the UK, one immediately has the information which leads one to the third jurisdiction. We will return to this scenario later to determine what evidence should be requested.

2 OECD Glossaries. Corruption: a glossary of international standards in criminal law – ISBN 978-92-64-02740-4-OECD 2008 at page 30.

Vehicle ownership

Another major lead that one has from the pre-investigation activities is the ownership of an USD 80,000 Mercedes by the wife. The fact that the Deputy Minister's wife owns an expensive automobile is an indication that he may be living above his means. However, the more important question is how the USD 80,000 was paid. This will involve first tracing the ownership of the car to determine the prior owner. In this case, one determines that the vehicle was purchased from the local Mercedes dealership. The records of this transaction indicate that the Deputy Minister was the purchaser and the date of the purchase. Is this enough information? The answer is no. The most important piece of evidence is to establish the source of the payment. If the payment were made by bank cheque, the dealership may have a copy of the cheque. However, if the files do not contain a copy, it may be necessary to obtain this information from the dealership's bank where the cheque was deposited. If the payment was made by cash, this is a an interesting piece of evidence since one's cash analysis of his bank account established that he did not have available cash in the amount of USD 80,000 from his legitimate sources of income.

Award of sole source contracts

The pre-investigation also disclosed that the Deputy Minister's office has awarded 23 sole source contracts in the last three years for infrastructure development projects, totalling in excess of USD 195 million. The government procurement rules for country A require competitive bids on all contracts over USD 100,000 unless certain conditions are met that are provided in the exception rules which are very strict. Each of the 23 sole source contracts will need to be analysed to determine how they qualified for the exception, who approved the contracts, how other potential bidders were disqualified and the personal involvement of the Deputy Minister in each situation. This will often require employing the services of someone who is an expert in government contracting procedures to assist in the analysis of these files.

If managers below the Deputy Minister's level approved the contracts, it may be necessary to analyse their promotion history and perform a brief review of their assets. For example, if the person approving the contracts received three promotions by the Deputy Minister in the past two years, this could be an indication that he owes favours to the Deputy Minister. This situation would require further investigation. In another instance, it may be discovered that the approving official has acquired assets that are beyond the scope of his legal income. It may be fruitful to trace the purchases of these assets to determine the source of the payments. Possibly the Deputy Minister is providing funding for the subordinates' asset acquisitions. All possibilities must be considered to determine the reason for the sole source contract awards.

IV. Results of the investigative inquiries

The Deputy Minister's personal residence was purchased just two years ago, and he has over USD 500,000 in equity. How did this occur? The investigation has disclosed that the Deputy Minister made an initial down payment in the amount of USD 540,000 on the house. This payment was received from a lending institution in the United States (US). Did the Deputy Minister really obtain a loan from a US company? What collateral did he give for such a large loan? Further investigation through the MLA process reveals that the loan was actually guaranteed by a company that received a large contract through the office of the Deputy Minister. This company, which is located in country A, has also been making each of the monthly loan payments. What questions should be asked when the representative of this company is required to

submit to an interview? One area of great importance is to determine how the company recorded these payments to the loan company in the US in its internal records. There are very few legitimate reasons why a company that was awarded a large contract through the Deputy Minister's office is making payments on a loan for the benefit of the Deputy Minister. These payments certainly have the appearance of a potential bribe. There is a high probability that the company records will disclose a false accounting entry such as listing the payments as a 'bonus' or 'research cost' or 'consultant fees'. Further investigation of the company records and related interviews should prove the true nature of these 'bribe' payments.

Information from the universities in the UK also yielded interesting information. The police in London were able to obtain informal intelligence that the tuition payments were made by a subsidiary company of a corporation that was awarded a USD 35 million contract through the Deputy Minister Deputy Minister's office. This company is located in a separate jurisdiction that will require a formal MLA request to compel testimony from the company officials and to obtain copies of their accounting records. Prior to submitting this MLA request, a preliminary call should be placed to the officials in this country to establish the communication links. It would also be advisable to ask if law enforcement officials from country A could participate in the interview with the company officials. The investigator will have the most information about the details of his or her case and is best prepared to ask follow up questions and to pursue leads developed through the answers provided. The investigator's presence at the interview in this foreign jurisdiction will, of course, only be possible through invitation by that country.

The Mercedes was purchased for USD 80,000 and the payment came from a loan company in Guernsey. Subsequent investigative efforts through MLA requests revealed that the loan company was merely a shell entity with a bank account. Deposits to this account came from another corporation that was awarded a contract by the Deputy Minister's office.

V. Conclusions

The investigation is certainly not complete at this point. There are many additional inquiries that need to be made. All payments from companies to the benefit of the Deputy Minister must be pursued. Company officials will be interviewed, accounting records analysed and all banking transactions completely traced. This will most likely identify additional assets acquired by the Deputy Minister, many of which will be in nominee names or hidden in corporate structures. Following the money will lead the investigator to these.

The investigation also disclosed that personal expenses for university costs were paid by similar companies. Taking further investigative steps following the money trail will yield additional evidence of apparent bribe payments. These money trails will not always lead directly from the private sector bribe giver to corrupt government officials. Sometimes, the payments will be clouded by numerous shell companies, trusts and nominees. However, the concept of following the money will usually lead to the beneficial owner of the assets and the maze of companies, trusts and nominee owners can be pierced through the complete financial investigative process.

Hidden assets will generally not be identified through commercial database searches and open source information. The information that the corrupt official wants to hide will often be concealed through complex financial structures established by skilled lawyers and accountants. In most cases, the financial investigation will be the best method of identifying the proceeds of corruption and making the connection to the corrupt activity.

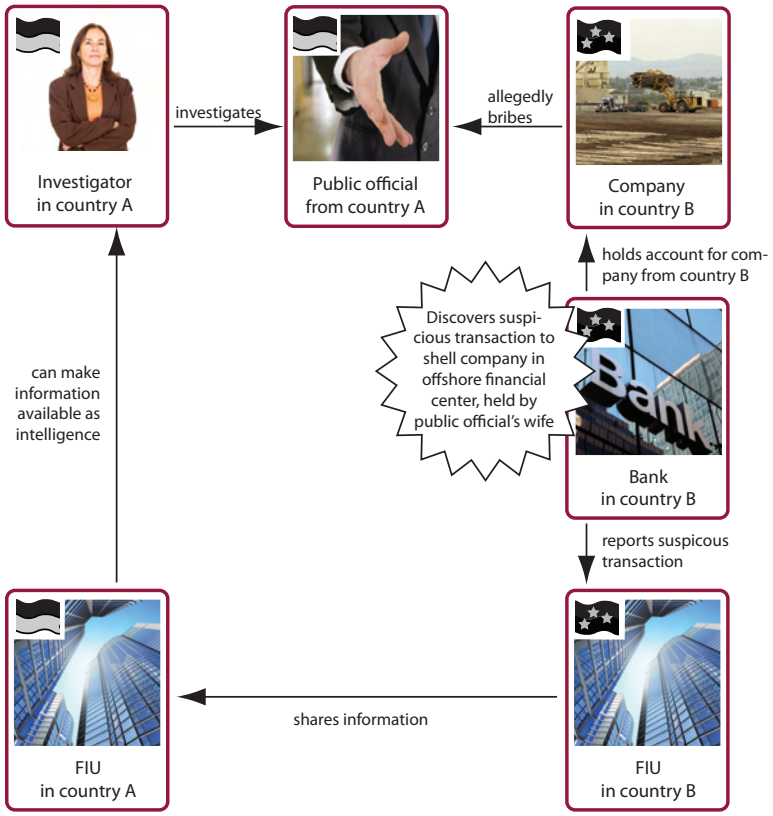
DANIEL THELESKLAF*

Using the anti-money laundering framework to trace assets

I. The potential

An investigator in country A is investigating a senior public official for receiving a bribe from a large European based construction company in country B. For many years, it has been impossible to secure evidence that the public official has received a bribe from the company, and the investigator is about to consider closing the case. At this point, a bank holding an account for the European company reports on a suspicious large transaction to an offshore company allegedly owned by the wife of the public official under investigation. Can this piece of information rescue our investigator's case?

Cooperation between national Financial Intelligence Units



* Daniel Thelesklaf is a lawyer by profession and Co-Director of the Basel Institute on Governance. After a career in the private sector at Swiss Life and Dresdner Bank, he joined the Swiss Federal office of Police in 1998 to become the first Director of Switzerland's FIU.

II. The anti-money laundering framework

The international Anti-Money Laundering (AML) framework has been expanded significantly over the last 20 years. Starting from a small group of Organisation for Economic Co-operation and Development (OECD) countries, standards have been established on how countries can fight money laundering. These standards are now in the process of being implemented in over 100 countries, including all major financial centres.

The goal of a large number of criminal acts is to generate a profit for the offender who carries out the act in question. All over the world, these offenders do not wish for law enforcement agencies to detect the proceeds of their criminal activity. In all too few cases where a law enforcement agency manages to identify proceeds of crime, these criminals do not want to be associated with these assets. This explains why offenders and many professionals offering their services try to launder the proceeds of crime – to disguise the illegal origin. Money laundering is, in a nutshell, the conversion or transfer of property, knowing that such property is derived from a serious offence, for the purpose of concealing or disguising the illicit origin of the property. Corruption offences belong to the category of serious crimes that have to be considered as predicates offences for money laundering, according to the international standard.

> Money laundering =
> Conversion or transfer of property derived from a serious offence, for the purpose of concealing or disguising the illicit origin of the property

The Financial Action Task Force on Money Laundering (FATF), based in Paris, France, is considered to be the main international AML standard setter. Over the last 20 years, FATF has developed a comprehensive set of recommendations on how countries should fight money laundering. Some areas of the international standards will be reviewed in this chapter, especially in relation to law enforcement and international cooperation issues, financial institution secrecy laws and certain aspects of the preventive measures.

The current international AML framework consists of the following main elements, relevant for asset tracing purposes:

- The criminalisation of money laundering
- The due diligence measures for financial institutions and designated non-financial businesses and professions
- The requirement to report suspicious transactions to the Financial Intelligence Unit (FIU)
- The record keeping requirements
- Supervision of financial institutions and designated non-financial businesses and professions (DNFBPs)

Each element has to be considered individually to identify the potential for use by investigators in tracing stolen assets.

1. The criminal offence of money laundering as a weapon to trace assets

By increasing the cooperation of employees of financial institutions in a criminal investigation

Anyone can be a money launderer and assist criminals to disguise the origin of the proceeds of crime – even the offenders themselves when they launder the proceeds of their own crime. One category of individuals remains the focus of the criminal offence of money laundering: individuals working in financial institutions and dealing with other people's assets. If they know, or if they must assume, that the assets entrusted to them are proceeds of (serious) crime, and do not refrain from accepting or transferring them, they will be held criminally liable. From an investigator's point of view, this opens up radical new ways on how to identify assets. It is unlikely that employees of financial institutions will offer their spontaneous assistance in investigations – this is not the role of financial institutions and their employees. But, in all honesty, the employees of a financial institution do not want to become involved in an investigation or prosecution. Reminding them of their possible criminal liability for money laundering can be a powerful tool for ensuring employees of financial institutions cooperate with law enforcement during the course of an asset tracing investigation.

By increasing cooperation of financial institutions

FATF recommends that countries should introduce criminal[1] liability for legal persons. Legal persons should be subject to effective, proportionate and dissuasive sanctions if their employees commit money laundering and the financial institution does not have an effective preventative system in place to avoid such criminal activity. The United Nations Convention against Corruption (UNCAC Article 26) insists on the same standard, also for money laundering. As of 1 September 2009, 136 countries have ratified UNCAC.

From the investigator's point of view, this new offence will open an additional door to trace assets. The threat of a criminal investigation against a financial institution is massive – the institution will not only risk a criminal sanction, more importantly, it will likely be subject to an administrative procedure by the relevant supervisory body. To increase the quality of the financial institution's defense against such actions, it will become more cooperative, and may lead the financial investigator to assets that have been outside of the scope of the investigation so far.

By using money laundering investigations in a financial centre as an indirect way for mutual legal assistance (role reversal between requested and requesting state)

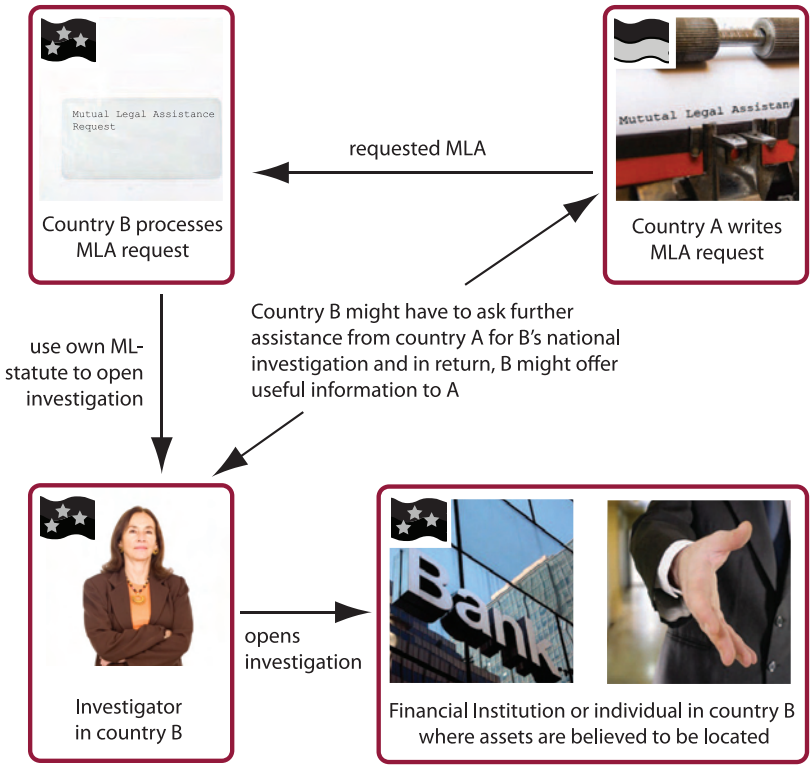
A mutual legal assistance (MLA) request sent to a financial centre seeking assistance in tracing the proceeds of crime can be a frustrating experience for a requesting state. The requirement disallowing 'fishing expeditions' can become an obstacle to identifying the proceeds of crime. The fact that, in many financial centres, decisions to render MLA can be challenged by the account holders in court, will further slow down the process.

These obstacles can be overcome if – after having received a MLA request (from country A in our opening scenario) – the requested state (country B) uses its own money laundering statute to open an investigation against an individual or a financial institution, where the assets are believed to be. This procedure may lead the financial centre investigator to a situation where he or she would have to request information

1 Or administrative or civil liability, where criminal liability is not possible (FATF Recommendation 2).

from the country that originally forwarded the MLA request. To substantiate this second MLA request, the financial centre (country B) investigator would have to consider offering information to the country where the predicate offence had its origin (country A). These pieces of information, contained in the second ('reversed') MLA request can become important leads to feed the original investigation.

'Reverse' Mutual Legal Assistance



2. The due diligence measures for financial institutions and designated non-financial businesses and professions

The due diligence requirements[2] imposed on financial institutions and DNFBPs[3] include:

- The identification of the client and the verification of this identification
- The identification of the beneficial owner[4] and taking reasonable steps to verify the identity of the beneficial owner
- Obtaining information on the purpose and intended nature of the business relationship

2 FATF Recommendation 5.
3 E.g., lawyers, accountants, tax advisors, dealers in precious objects, casinos, real estate agents.
4 Beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.

- Conducting ongoing due diligence on the business relationship

The documents the financial institution must collect to meet the requirement that information on the purpose and intended nature of the business relationship must be obtained, can become a very valuable source of information for the investigator in tracing business relationships that have not yet been detected in the course of the investigation. Often, these documents will summarise the financial situation of the client, contain information on other or previous business relationships with other financial institutions or contain the letters of introductions of lawyers or accountants. These pieces of information are all potential new leads.

A good investigator knows precisely the nature of requirements of financial institutions arising from the AML Laws and Regulations. This knowledge allows him or her to ask the right questions, and request production of the right documents, such as background reports on the individual business relationship.

Large financial institutions can only meet the obligation to conduct ongoing due diligence on the business relationship by using Information Technology (IT) based transaction monitoring systems. These systems are designed to flag potentially suspicious transactions as part of the financial institution's AML program. Such systems inevitably produce many false hits but the financial institution is required to analyse these transactions. This analytical process will often include additional information requested from the client. This additional information will, in turn, give a more detailed picture of the client's financial situation and the type of business he is conducting. These 'background memos' trying to clarify and justify unusual transactions are another potentially interesting source of information for the investigator.

3. The requirement to report suspicious transactions to the Financial Intelligence Unit (FIU)[5]

Probably the most interesting tool for an investigator in tracing assets, especially assets stashed away in financial centres, is the requirement obliging financial institutions and DNFBPs to report suspicious transactions to the national FIU.

In most financial centres, financial institutions and DNFBPs have to file a suspicious activity report (SAR) if the assets the suspect entrusted to them originate from a predicate offence.[6] Corruption offences are mandatory predicate offences to money laundering. What does that mean for a Police Officer, Magistrate or Prosecutor investigating corruption, who believes that the suspect has stashed away the proceeds of the corruptive act in a particular financial centre? Most often, the investigator will not know which financial institution is involved. In Switzerland alone, there are 400 banks and nearly 10,000 non-banking financial institutions. A request for information from the Swiss MLA authorities without being able to name the financial institution involved would be considered as a 'fishing expedition', and returned to the sender.

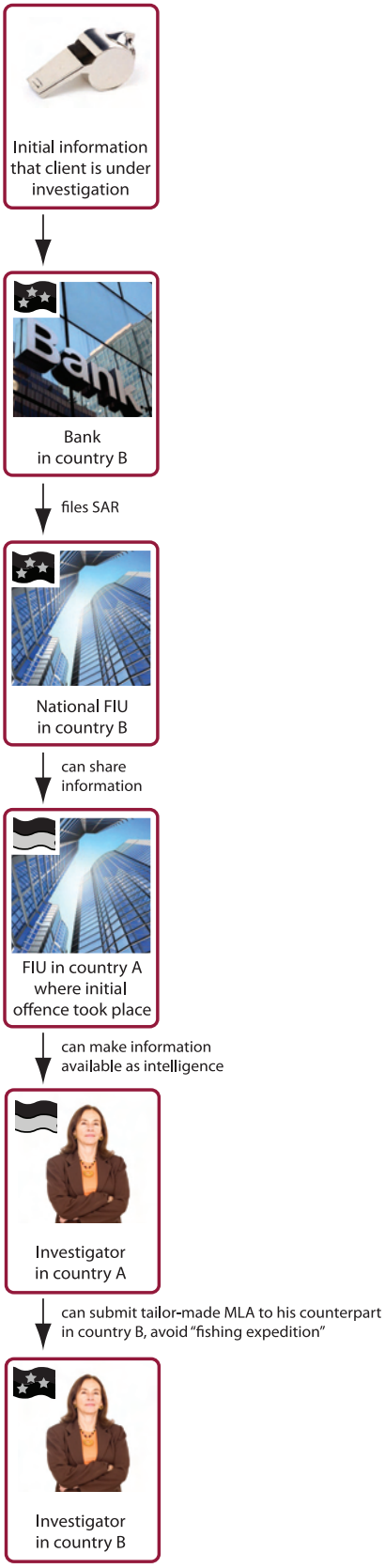
How can we overcome this obstacle? Once again, the AML framework may prove to be of assistance: A bank is likely to file a SAR in respect of a client if the information reaches the bank that the bank's client is under investigation for a predicate offence to money laundering. Once the SAR is with the FIU in the financial centre concerned, this FIU can share information with its counterpart FIU in the country where the predicate offence took place. Under certain conditions, this information can be made available to the investigator in the country where the predicate offence occurred

5 FATF Recommendation 13.
6 E.g., Art. 9 Swiss AML Law, Art. 17 Liechtenstein Due Diligence Law.

(normally as intelligence only, not as evidence). This allows the investigator in question to locate the stolen assets and submit a tailor-made MLA request to his or her counterpart in the financial centre and avoid the problematic 'fishing expedition'.

However, to prompt an SAR, the financial institution in the financial centre must learn about the predicate offence in the country of origin of the crime in some way. In corruption cases, the country of origin is very often a developing or transition country with limited law enforcement capacities. Financial institutions will not regularly access news from developing or transition countries. Only a few major banks' compliance officers would systematically read newspapers and screen them for potential allegations against clients. So, the information on an ongoing investigation must somehow be spread and reach the financial institutions in financial centres. There are various mechanisms for ensuring this information can be spread, either by using existing contacts in the financial centre – networking is of crucial importance for successful asset tracing – or the international media in cases of high profile investigations. Or else specialists can be found in financial centres that target major financial institutions, and provided with case related information that is not confidential but sufficient for the financial institution to consider filing an SAR.

The requirement to report suspicious transactions



The record keeping requirements

All individuals and entities subject to the relevant AML legislation (financial institutions as well as DNFBPs) are required to keep records:[7]

- For at least five years, on transactions, both domestic and international, in order to comply swiftly with information requests from competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency)
- For at least five years after the business relationship has ended, in respect of records on the identification data obtained through the customer due diligence process, account files and business correspondence. This may include copies of official identification documents like passports, identification cards or similar documentation

The identification data and transaction records should be available to domestic competent authorities upon appropriate authority. A failure to keep these records must be subject to a sanction (criminal or administrative).

Supervision of financial institutions and designated non-financial businesses and professions (DNFBPs)

All individuals and entities subject to a country's AML legislation (financial institutions, as well as DNFBPs), are subject to oversight by the relevant state body. These supervisors have considerable influence on the behaviour of financial institutions. Very often, a financial institution will first try to address the requirements of the supervisor before thinking of the risk of a potential criminal investigation. The number of criminal convictions of employees of financial institutions for money laundering is still low. Avoiding problems with the regulator is an incentive for a financial institution that can be used to advantage by an investigator.

In countries where the supervisor puts emphasis on the implementation of AML legislation and regulation, investigations can benefit from this policy by:

- Working closely with the supervisors by providing them with information on the constraints and challenges in investigating cases where supervised entities are involved, with a view to allowing the supervisor to remind the supervised entity of its obligations
- Educating the supervisor's staff on patterns of money laundering, to improve the quality and results of the supervisor's on site inspections
- As an *ultima ratio*, transferring cases to the supervisor for non-compliance with the AML legislation. Naming and shaming of financial institutions for non-compliance with AML legislation often has a greater effect than the criminal investigation.[8]

7 FATF Recommendations 10 and 12.

8 A good example is the report of the Swiss regulator in the Abacha case. Several banks have been named and fined for non compliance with the AML Regulation. Find the report on: http://www.finma.ch/archiv/ebk/e/archiv/2000/medien2000.html.

III. Conclusion

The international AML framework, once properly implemented in a country, has huge potential for use by investigators and prosecutors in locating and tracing assets of criminal origin. However, the investigator and prosecutor should be well aware of the requirements of the relevant AML laws. A good investigator or prosecutor should also reach out to his or her country's FIU and all supervisory bodies to facilitate the successful investigation of asset tracing investigations and ultimate court proceedings in this regard.

HARI MULUKUTLA* AND MARKUS RÜEGG**

The importance of Information Technology in tracing stolen assets

I. Introduction

Information Technology (IT) plays a crucial role whenever systematic and proven techniques have to be employed in conducting financial investigations and in constructing the money trail in cases involving stolen assets. A successful investigation can only be carried out with the proper tools and processes to detect and investigate the elements of the crime in general, and in cases of fraud, corruption and financial crime in particular. Increasingly, the investigation process of corruption cases, inclusive of asset tracing, involves the collation and analysis of large volumes of financial and other data. When conducting financial investigations, a good IT tool is a must. Without an IT system, the financial investigator will be looking for the proverbial 'needle in a haystack'. The types of data collected can include bank statements, telephone records, registration documents of vehicles and property, tax records, company records, invoices, bills, receipts and data that is stored solely on computer hard drives, sometimes requiring forensics[1] and reconstruction of encrypted files and other law enforcement records. The investigative case file is developed further using information gleaned from collected evidence, and intelligence gathered from public domain sources. This collection of heterogeneous data can be combined within a single information management system to eventually reconstruct the money trail, including the entities and channels used for stealing and hiding the assets.

The use of IT tools in the tracing of assets offers many benefits. For example, the use of a case management system will make it easier to use systematic and repeatable processes in the identification, location and recovery of stolen assets. IT systems[2] are also essential for cooperation and information sharing between law enforcement and regulatory agencies, and financial institutions that have a reporting obligation. Such cooperation inevitably has a human component but the technology makes it possible to

* Hari Mulukutla is a business process and information systems professional focussing on governance, anti-corruption and stolen asset recovery, providing expertise to important stakeholders in both the public and private sectors.

** Markus J. Rüegg is an Analyst and IT Officer in the Financial Intelligence Unit, Principality of Liechtenstein.

1 Computer forensics, sometimes known as digital forensics, is a branch of forensic science pertaining to legal evidence found in computers and digital storage media. 'Forensic' implies 'suitable for use in a court of law'. In criminal investigations and legal cases, computer forensic techniques are frequently used to analyse computer systems belonging to defendants and those in custody.

2 Recognising the importance of IT by allocating sufficient resources is critical for a successful strategy. For example, according to a report on ZDNet (11 December 2008), the United Kingdom's Serious Organised Crime Agency (SOCA) was preparing to embark on a GBP 500 million (USD 742.6 million) project to integrate its IT systems to bring together around 50 systems, which the agency inherited from a variety of agencies such as the National Crime Squad, the National Criminal Intelligence Service and part of the investigation arm of HM Revenue and Customs.

institute simple and secure measures to share intelligence and 'law-enforcement' type information.

In 'following the money trail', investigators need accurate, reliable, comprehensive and up-to-date information on a global level. There are many watch lists, sanction lists and risk databases which assist the investigator in developing a comprehensive personal profile of an individual/entity. This real time access to such information, in turn, assists the investigator in linking the individual/entity to the assets under investigation and even, in many cases, to the crime itself. Technology is not a magic bullet for asset tracing. The detailed and methodical work which can sometimes get complex very quickly must still be done to make progress in the investigation. Therefore, the key components of a successful strategy to identify corruption cases and obtain the leads to trace stolen assets are people, process and technology. Investigations should be focused in terms of resources deployed and guidelines followed. This includes utilising staff in the most cost-effective manner and developing terms of reference that contain a comprehensive list of all the necessary resources (human, financial or material) for a successful investigation. A policy document that includes a clear description of the facts that have given rise to the investigation and all decisions made during the investigation, along with the necessary justification, is also a useful tool for the investigation team. This chapter focuses on providing the investigator with a basic understanding of the process and tools which can be deployed during the pre-investigative and investigative stages of any investigation aimed at identifying and locating stolen assets.

II. People, process and technology

Technology forms an important pillar of the three essential components in implementing a successful asset tracing strategy: human competencies, processes and technology. The human competency is an absolute essential. An investigation team must have the expertise and skills required to conduct asset tracing and financial investigations. For cross-border tracing of stolen assets, financial investigators need to seek international assistance from their foreign counterparts and, hence, they need to know the requested country's legal system and procedures in place to receive assistance. Most countries require that requesting parties furnish evidentiary documentation that is secure and foolproof. The second pillar is the process. High level processes, structured according to tasks and checklists have to be developed and disseminated to the investigating teams. This process oriented way of doing the work will create institutional knowledge that can be developed, recorded and harnessed for future use and training. The third pillar, the technology component is essential to develop the processes, systematise them and store them in an IT system that can be easily accessed and essential information shared by the investigators and other law enforcement agencies while at the same time maintaining data quality, integrity and security. This three pronged approach of using people, process and technology for the tracing of stolen assets will achieve more reliable and predictable results, and makes the best use of resources committed to the investigations.

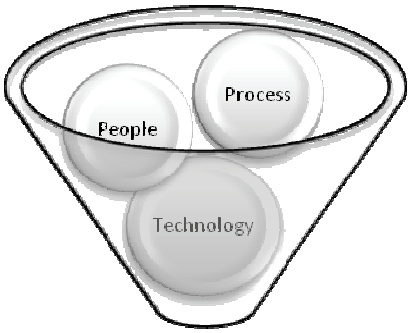


Fig. 1: The three components required for an information technology strategy to perform asset tracing.

III. The intelligence cycle

A process oriented law enforcement setting needs to incorporate several steps to cover all aspects of the intelligence cycle including the planning, collection, evaluation, analysis, reporting and dissemination of the intelligence data. The information is reviewed at each stage for quality, accuracy and timeliness. Automation cannot replace the expertise that comes from training and professional experience. However, the use of information systems incorporating the various stages of the intelligence cycle and the review and monitoring of the data greatly reduces the burden of work and errors, and increases reliability. The intelligence cycle requires the investigator charged with tracing of assets to ask a number of questions before determining the course of action. The various facets comprising the intelligence cycle should be carefully considered and documented in order to guide the asset tracing investigator. The following list of questions will assist in formulating a comprehensive and detailed intelligence cycle.

Steps for analysing and documenting the intelligence cycle:

- What type of cases will be covered by the intelligence cycle?
- What is the relevant legislation that is applicable for asset tracing?
- What is the relevant legislation required for cases with an international dimension?
- How does a corruption investigation begin?
- What are the steps in the various phases of the lifecycle of a case?
- What channels of information trigger a pre-investigation?
- What are the required processes in the investigation phase?
- What are the required procedures to bring a case to prosecution?
- Who leads the investigation, police and investigators or prosecutors?
- What are the roles and responsibilities of individuals working on a case?

Following the steps outlined in each phase of the intelligence cycle, the investigator then has to record a number of pieces of documentation: complaints, evidence, testimonies and related information. As one can imagine, this information can quickly grow to a large size and become increasingly complex to manage and refer to. This brings us to a discussion of case management systems which is explored in the next section.

IV. Case management systems

A Case Management System (CMS) is used in a variety of law enforcement settings to facilitate the recording of case proceedings and evidentiary documents within an IT database, enabling information sharing internally within an agency and between agencies that comprise the criminal justice system. A basic capability of a CMS is to facilitate tracking and reporting of cases. In the case of an investigative agency, a CMS provides a high level overview of the number and status of ongoing cases (e.g., number of cases being investigated or prosecuted and the personnel working on them etc.). A further function of a CMS is to mirror the workflow process of a case from the receipt of an allegation or complaint through pre-investigation and investigation, prosecution and the eventual outcome (judgments, sentences) of a case and, where applicable, the asset tracing recovery proceedings. The benefit of a CMS following the lifecycle of a case is that it can serve as a tool to facilitate the handling of cases in a systematic fashion, their progression from one stage to another stage with the appropriate approvals, and in addition, the management and monitoring of personnel allocation for a case, e.g., across the region or nationally.

Fig. 2: Benefits of a using an automated computerised case management system

The CMS achieves a higher level of sophistication by incorporating features such as:

- Facilitate the sharing of information. For example, it could provide the capability to store and readily access data related to a case such as a synopsis of a case, witness statements, records of interviews and evidentiary documents.
- Facilitate the investigation process. For example, it can have access to third party agency data sources such as Citizen Identification (ID) lists, property and land registry databases, police electronic records of arrests/convictions, Court Dockets, Office for Foreign Asset Control (OFAC) lists, etc. These data sources can be used to assist investigators and prosecutors in obtaining background information early on regarding individuals and companies, and link information about individuals and companies across cases in a secure manner which preserves the integrity of the investigation and prosecution.
- Provide a methodical process flow with checklists and steps required by legislation and best practice, in an investigation or prosecution. For example,

there are certain recommended steps to perform when an investigator is trying to obtain International Mutual Legal Assistance (MLA). The CMS could either have 'How To' guides embedded in the system that provide guidance, or it could require the investigator to answer a series of questions to record that certain tasks have been performed. These examples of more complicated CMS capabilities come with a cost in terms of time to design, develop and implement. Eventually, this could, however, lead to a dynamic process tool.

- Prevent unauthorised tampering (i.e., removing, replacing, etc.) of files, ensuring the integrity of evidence with system-wide audit trails.
- Introduce advanced analytics including trend spotting, efficiency assessments and comparative analysis.

Fig. 3: Shows increasing complexity of a CMS beginning with a baseline system with minimal features to a full blown investigative tool with workflows spanning multiple agencies and sharing of information across cases.

1. Audience for a CMS

CMSs are useful to a number of organisations, ranging from anti-corruption commissions, investigating agencies, prosecutors to the judiciary.[3] The nature and function of the systems can differ widely from organisation to organisation depending on what the system is used for. An investigative agency will store the evidence and leads and organise the case data in an electronic and secure content management system. They will need to update the case as it progresses through the intelligence cycle. However, a court case management system may only track the progress of the case the moment it is scheduled for hearing. No evidentiary documents or testimonies are stored and disseminated but just the schedule, the case status, caseload, etc. are tracked in such a system. Prosecutors, on the other hand, will use a CMS to prepare a whole case docket with all the required documentation to bring it to trial. The point that must be mentioned here is that all these different agencies could be using different systems but they have to be inter-operable and data in some form should be exchanged otherwise the benefits of electronic case management cannot be fully realised.[4] The

3 Increasing the effectiveness of courts can reduce both the incentives and opportunities for judicial corruption. Measures that typically fall within the ambit of 'institutional strengthening' include: Introducing information and communication technologies, including case management systems; U4 Brief: UNCAC and Judicial Corruption, September 2009.

4 A classic problem plaguing Indonesia's Criminal Justice System is the chronic lack of coordination within the system, particularly between the police and the state prosecutor's office (Fast-tracking Anticorruption Management, The Jakarta Post, 18 June 2007).

use of a well-designed and inter-operable CMS for effective management and tracking of cases while ensuring the integrity and security of case data is hence essential.

2. Steps for CMS adoption

New organisations adopting IT systems for case management have to undertake a series of steps:

- Perform a needs analysis and create a business case for deploying a CMS in an organisation
- Identify stakeholders and gather requirements, perform business analysis and develop use cases
- Document workflows and case processes
- Improve the processes with best practices: process streamlining
- Obtain management support and funding
- Create specifications for a working prototype
- Identify partners or vendors that offer CMS solutions: pilot a sample system
- Develop or customise an off-the-shelf solution
- Deploy solution and train users
- Survey usage, obtain feedback and fine-tune system to meet requirements
- Start with a simple solution and deliver increasing complexity and features in phases over time and after usage
- User participation from an initial stage is critical for successful implementation
- Develop migration plan for data from legacy systems, including strategies how to incorporate paper-based data into the CMS

3. Technical pre-requisites for CMS adoption

A basic IT set-up is required to implement IT-based CMSs consisting of the following:

- A high-availability, fault-tolerant and secure computer network is required for an IT CMS to be deployed
- Secure e-mail and collaboration systems. Often e-mail and daily work calendars are an essential information component that reflect day-to-day activities in respect of a case. These have to be integrated into the CMS. E-mail communication has to be archived as part of the chain of custody
- Adequate server hardware capacity to support the user base, and provide quick access to information, archival facility and backups
- A reliable and secure operating system and software technology that support open standards for data exchange and inter-connectivity
- Trained IT personnel or a service provider to design and deploy a CMS, train and support the user base

A range of activities is necessary to plan and organise a CMS. The streamlining of existing manual and computerised processes must be initiated, procedures documented and the technical issues associated with implementing a CMS defined: information system, storage, retrieval, archival, security, computer networks, hardware/software,

capacity to record evidence and other case information digitally and securely, providing role based access control. The role of shared documentation spaces to help collaboration and training must be discussed, and solution design, technical architecture, project implementation plan, budgets, consultants, product vendors and expert resources which are required, initiated. The following steps describe the considerations in further detail:

- Evaluate and list all business processes (manual processes, information registers, dockets etc.)
- Information communication technology (ICT) infrastructure - architecture, design, procurement, implementation with security considerations (secure e-mail, secure file sharing and collaboration, secure access to databases and case files, evidence, case dockets, etc.)
- Electronic access to legal databases, case law, sentences, court records, court calendar. Access to other databases on individuals, real estate, properties, vehicles, biometric data, if available, that can be used by prosecutors while guiding an investigation
- Technical architecture of how all these databases can be created and accessed securely on proper communication and network channels
- Choice of technologies, vendors, consultants, governance of projects and project management
- Use of best practices: software engineering principles and processes
- Case management functions (preparation of documents, office work automation, work flow, notifications, reminders for court dates, shared team calendar, general statistics and caseload statistics and management reports)
- Inter-operability issues: integration and flow of information between the investigators/prosecutor's office and with other judicial levels such as the court of appeal; and integration across branches of the criminal justice system and law enforcement such as police/intelligence, prosecutor's offices and judiciary

High profile corruption cases often require the compilation of an MLA request for multi-jurisdictional and international cases – a CMS will enable quicker turn-around and standardisation of sending and receiving international requests.

V. IT tools for analysis, visualisation and charting

Financial investigations and asset tracing typically involve the analysis of vast amounts of raw data that is unstructured and produced in various formats. This data may contain important intelligence information which is not immediately apparent. Several important facts and financial transactions belonging to persons and companies of interest may be buried in the volume and randomness of the data. To be able to analyse this information, the investigator needs IT tools to capture and organise the data, visualise the links and hidden information and convert it into actionable leads and admissible evidence. There are several well-known analysis and visualisation systems and tools available in the market that enable investigators to understand complex cases, generate visual charts and reports, and reveal hidden connections from structured and unstructured data such as phone records, bank statements, travel documents, e-mail messages etc.

A prerequisite for successful analysis is the availability of data in digital form. Very often, however, the investigator is faced with paper-based data. Telephone companies in the jurisdiction may not make telephone data available digitally, information obtained through legal assistance channels may arrive in the form of photocopies, faxes and seized bank records may consist of thousands of paper documents. In such situations, IT tools for digitising data, such as, for example, Optical Character Recognition (OCR) software, and transforming the data to a format suitable for analysis will become indispensable.

The data analysis requirements of a financial intelligence unit (FIU) are a good example of the processing of large volumes of data. Banks and other financial and non-financial institutions have reporting obligations, and the reports are typically submitted as suspicious activity reports (SARs) or suspicious transaction reports (STRs) as the case may be according to the country's laws. In many instances, the information is sent automatically from the financial institutions or via the central bank to FIUs. In addition to the suspicious transaction/activity reporting, if a threshold model is adopted, all transactions over a certain monetary value have to be automatically reported to the FIU. In such cases, the volume of transactions is so high that an elaborate IT system involving database software supported by adequate computer hardware is essential. This data is collated, processed and fed to the analysis tools. The case file is also enriched with information from classified and unclassified data sources such as law enforcement data, public domain information, previous SARs, international cooperation, etc. It would be virtually impossible to glean intelligence information from such large datasets without the deployment of analysis and visualisation tools.

The analysis and visualisation tools must also enable the investigator to slice and dice the data from a high level overview to small detail, discover associations, communication trails, money flows, perform timeline analysis to reconstruct events and transactions over a specified time period, and view the data from different perspectives and the unique requirements of the case.

Fig. 4: Analysis: Data Collection, Retrieval, Visualisation and Reporting

VI. Forensic Technology

The complex set of tasks in an asset tracing procedure using legal remedies can be greatly supported by making use of computer forensics tools. Technology has allowed traditional criminal activity to flourish and conceal stolen assets, transfer those assets abroad quickly using online banking tools and destroy evidence. Most of the online transactions, however, do generate an electronic trail of evidence. Forensic acquisition and analysis of data allows the combination of lost and tampered data with other digital evidence to increase the admissible and available evidence to assist in

reconstructing the money trail. These tools allow for easier identification, collection, preservation, analysis and presentation of evidence generated or stored in a computer. Computer forensics typically uses a systematic approach to mining the large volumes of electronic information to provide benefits such as:

- Increasing the available datasets for analysis and investigations
- Recreation of data that was intentionally or accidentally destroyed from computer disk drives, flash memory devices and other storage media
- Securing and analysis of large volumes of email
- Countering encryption and data security

Additionally, as much of the day-to-day communication and financial transactions are conducted over the Internet, real time monitoring of bank accounts, e-mail traffic and the interception and processing of other forms of on-line data become essential to conducting a proper investigation, complementing traditional investigative and surveillance techniques. This type of monitoring can be done only to the extent allowed under the legal requirements of the jurisdiction involved, e.g., search warrants and data privacy rules.

VII. Public domain intelligence gathering to trace stolen assets

1. Semantic Technology

Often, publicly available information and classified law enforcement information have to be combined and the aggregate converted into intelligence for investigations and the asset tracing process. An emerging technology is the concept of the semantic database and the semantic web. Traditional data mining[5] techniques such as association analysis, classification and prediction, cluster analysis, and outlier analysis identify patterns in structured data. Newer techniques such as semantic analysis identify patterns from both structured and unstructured data.

The information age provides anyone with Internet access with unprecedented access to a wide range of fast changing information. News reporting has seen revolutionary changes in how news is collected and rapidly reported on the Internet. This has tremendous ramifications for law enforcement and government agencies in the field of combating corruption, money laundering and recovering stolen assets. There is an ever-growing need to assess and analyse information that is circulated on the Internet, either via news channels, blogs or other informal methods of sharing information. Very often, the proceeds of corruption are transferred to a foreign jurisdiction very quickly over the Internet with the use of a few key strokes on the computer. Such capability poses additional burdens on the law enforcement and financial regulatory bodies. Agencies have to make the connection between information available publicly and information reported to them by financial institutions.

Semantic information systems consisting of state-of-the-art technologies from the field of Natural Language Processing (NLP) are being used in order to significantly enhance

5 Data mining is the process of extracting meaningful patterns from data. As more data is gathered and is available, data mining is an important technique to transform this data into useful information. Used everyday in a wide spectrum of data analysis fields, it is particularly critical for investigators in detecting corruption, fraud and the misappropriation of assets.

the results obtained from traditional information extraction methods such as keyword searches. In the semantic web, data is defined, stored and linked in a way to allow for the search and retrieval of information with higher accuracy, context based ranking of search results and integration with other systems with enhanced relevance.

For example, finding companies that appear on websites together with another entity is not directly possible through a simple Google Search – at least, not without prior knowledge of the names of the companies. The semantic technology, however, can automatically identify companies based on language grammar and rules, tag and store relationships such as links, as well as other relations like family relationships, roles and positions and monies or assets.

The semantic approach facilitates higher quality searches as the context of a keyword match is taken into account. For example, a traditional search for the entity or company name and 'Isle of Man' may yield many false positives – a number of websites contain the list of all countries in the world in order to allow a user to perform country-specific searches, or 'Isle of Man' may appear in an advertisement or in another, unrelated part of the page. The semantic database can be programmed with rules requiring, for example, that the entity name should occur with 'Isle of Man' in the same paragraph or sentence, or with more exact requirements such as 'doing business in' or 'is incorporated in' the Isle of Man. The semantic data repositories provide greater analytical power and make search queries more intelligent, based on relevance and meaning.

Asset tracing investigations can be assisted greatly by combining the semantic approach with the wealth of publicly available intelligence information from news websites, governmental watch lists, wealth disclosure reports of public officials and commercial data sources.

VIII. Conclusion

A number of areas dealing with IT and IT-based processes and tools for asset recovery investigations using both a traditional approach, as well as newer creative approaches, have been introduced in this chapter. There is growing evidence that successful financial investigative capacity for tracing stolen assets within a country requires a well thought-out and resourced IT strategy. The strategy consists of systematising the work, analysis of large volumes of data generated by financial institution records and transactions, law enforcement intelligence and commercial databases, thus fostering inter-operability and inter-agency coordination.

STEPHEN BAKER* AND ED SHORROCK**

Gatekeepers, corporate structures and their role in money laundering

I. Introduction

The financial world does not operate in one dimension. The traditional view that individuals hold direct, simple relationships with financial service providers is increasingly less relevant. This is especially so in a world of ever increasing complexity, driven by technological change and shifting political and social sands. Whilst the benefits of technological developments and globalisation have delivered benefits to many, it is also a double-edged sword. This is undoubtedly the case in the world of money laundering, which includes terrorist financing.

As criminals around the world have become alive to the opportunities afforded by the global economy to commit ever more ingenious crimes, so have they developed ever more sophisticated ways of concealing their illicit gains. They have not done so without assistance. Ever since the days of Al Capone, criminals have realised that it is not sufficient to simply be able to carry out the predicate crime and benefit directly from their activities. Law enforcement is likely to be able to quickly identify obvious linkages between ill-gotten gains and the criminal. It is for this reason that criminals place as much importance and invest as much time, money and effort into the manner in which their property is laundered and then used as they do in the crimes that generate that property.

At the core of these efforts lies the concept of achieving a 'disconnect' between a) the criminal and the proceeds of his crime; b) the proceeds of his crime and the form in which he ultimately derives his benefit and finally c) the criminal and his access to the benefit. These disconnects facilitate the safe enjoyment by the criminal of the fruits of his crime. However, a note of caution should be sounded about grouping terrorist financing with money laundering. Whilst there are many similarities between the techniques used by both, there are equally as many differences. The primary difference relates to the objectives of the terrorist versus that of the 'traditional' money launderer. The traditional money launderer is focused primarily on the retention of the proceeds of crime and subsequent access to his ill-gotten gains. The terrorist financier is focused on channelling what may be, initially, clean money into the hands of those who support his or her own ideological or religious beliefs. This may take the form of directly funding violent acts, but equally may centre around training activities, the promotion of beliefs or simply travel. In either scenario, gatekeepers have a role to play although experience has shown that terrorist financiers are primarily interested in using the banking system directly and capitalising on the speed with which funds can be transferred.

* Stephen Baker is an English barrister and Jersey advocate. He is a partner of BakerPlatt, a law firm based in Jersey, Channel Islands, specialising in litigation, financial crime and regulatory matters.

** Ed Shorrock, FCA is Director of Forensic & Regulatory Services at BakerPlatt, a law firm based in Jersey, Channel Islands.

None of this is achieved single-handedly. Money laundering schemes frequently employ a combination of gatekeepers and structures in order to achieve these disconnects. In this chapter concepts involved will be outlined.

II. Who are the gatekeepers and what are they hiding?

Gatekeepers, as the name would imply, are the people who facilitate 'access' to the world of financial services, enabling criminals to disguise their profits. These individuals and institutions are frequently bankers, corporate service providers (CSPs), trust companies, lawyers, accountants or other organisations which have access to the financial system. Depending on the precise nature of their role, gatekeepers commonly facilitate the following:

- Commission of a predicate offence – for example, the provision of a company owned by an overlying trust as a party to a fictitious contract or a contract that exists for an illegal purpose
- Disguising of a person's involvement in a commercial transaction – for example, disguising a principal's interest in a target company about which he has privileged information
- Layering of a criminal property – for example, passing property through the ownership of a company in an effort to place as much distance between property and the original criminal source, or
- Disguising of the ownership of property by the ultimate beneficial owners of that property

The typologies of such crimes are too numerous and detailed to describe in detail but they are all designed to achieve the 'disconnects' referred to above. A further reason for a gatekeeper's involvement is the provision of a veneer of respectability. Whilst a gatekeeper may, either intentionally or not, be involved in money laundering, the criminal's intention is that his role is to demonstrate to the banker, the lawyer or other players in the financial system, that his client is *bona fide*. The more respectable the gatekeeper, the more highly prized his services will be. The aim of the criminal is to ensure that he can put sufficient distance between himself and the proceeds of crime, whilst still maintaining a level of control over the assets, a topic which will be covered later.

A simple question may arise at this stage. Why would a gatekeeper permit the abuse of his services? The question assumes that the gatekeeper consciously acquiesces. That certainly occurs. Where it does, a gatekeeper commits a serious criminal offence. Their motivation is fuelled by greed and a risk benefit analysis (often aided by a lack of legislative and judicial infrastructure to prosecute these cases) from which they conclude that the chances of being caught are slim.

Of much greater academic interest are the factors that motivate gatekeepers to assist criminals unwittingly and without a guilty state of mind. Here, greed, the pursuit of profit or, at best, the need to meet revenue targets clouds judgement. Clouded judgement feeds the natural human tendency to want to believe what a client says, particularly if that client is 'valuable'. This 'human factor' applies across the financial services industry but is particularly prevalent within the 'professions' responsible only for structuring deals in circumstances where they do not become party to them. This lack of proximity can lead lawyers and accountants in particular to 'put the paperwork' in place without turning their minds to the legitimate rationale or usage to which the structures, deals and arrangements will then be put. The position is made worse still in

some cases by the perceived protection afforded both to clients and, ironically, to legal advisers by legal professional privilege. The protection afforded by privilege in such cases may, in fact, be a mirage, particularly in common law jurisdictions but it is still perceived to be of value by criminals.

Despite many changes in anti-money laundering legislation to promote a 'risk based approach', a key question often remains unanswered when gatekeepers accept clients and then facilitate transactions for them. That is – 'What is the legitimate commercial rationale for this relationship or arrangement?'

An interesting feature concerns CSPs. They offer a wide range of services including company incorporation, director services, nominee shareholder services, company secretarial services, registered office services and, of course, trustee services. At the top end of the market, CSPs are owned by private banks. They service the clients of those banks. The relationships with those clients are 'owned' not by the CSPs but by relationship managers, onshore. Numerous cases have shown that the pressure brought to bear upon the staff of private bank owned CSPs offshore, by onshore relationship managers to acquiesce to client demands, can be almost impossible to resist without careers offshore being damaged. At the bottom end of the market, CSPs are owner-managed and their business model relies on volume. Volume militates against quality and risk adversity. The more clients you have, the less likely you are to be able to conduct sufficient due diligence in respect of each. Frequently, CSPs offer 'trust and company packages' inclusive of registered office, directors, shareholders and book-keeping services for as little as GBP2,500. Employees of these companies sign 'legitimate' contracts on behalf of the companies they purport to 'manage and control' for very large sums of money and for little reward. Frequently they are not in possession of all of the relevant information to be able to make informed decisions on the risks.

1. Legitimate uses of trusts

The trust concept grew out of the practice in medieval England whereby nobles fighting in the Crusades would entrust their possessions to relatives or friends (the forerunner to the modern trustee) to provide for other family members in the event that they were killed in battle. The basic concepts still hold true today. There are a multiplicity of ways in which trusts are used legitimately. Estate or succession planning, tax mitigation and wealth preservation are the simplest examples of legitimate purposes, though trusts are also created to fund charitable goals.

2. The attraction of criminals to trusts and other offshore structures

Trusts and other offshore financial services are attractive to criminals because they make it more difficult to determine the true identity of the person who owns and effectively controls assets. A chief executive or chief financial officer may be diverting company profits to himself; an insider dealer may be tired of watching clients make money and may look to make a 'killing' of his own; a corrupt politician may loot his treasury for millions of dollars and seek to invest the proceeds through a trust. Even drug traffickers and ordinary fraudsters may seek financial services 'offshore'.

3. How trusts are abused

There are various ways in which a person will seek to disguise his involvement in illicit activities. The use of overseas limited companies and bank accounts in those

company names are very simple examples. Other methods are foundations, *Anstalts* and similar vehicles. However, trusts, and the various services offered by the trust industry, are a particularly good vehicle for criminal investments if those involved in such industries are not alert to the risks. In jurisdictions where trustees are not 'regulated', their vulnerability to criminal abuse is very high. The trust, and the ability to manipulate it, are indeed integral to the 'smoke and mirrors' a criminal uses to disguise ownership of property while retaining control over it. They can enable a criminal to achieve an effective disconnect (in terms of ownership) of property whilst enabling them to continue to exercise control and gain benefit.

The settlor

The precise method for routing funds into the trust structure will vary. A criminal may, for example, use a 'dummy settlor' to establish the trust with a nominal amount and to avoid identifying himself as the true originator of the funds in the trust deed. Numerous cases reveal that lawyers have been content to act as 'dummies' on behalf of their clients. In some jurisdictions a 'declaration of trust' obviates the need for a settlor to be named at all during the establishment of the trust.

The settlor will often sign a letter of wishes. This is a document, not legally binding on the trustee, which expresses the manner in which he wishes the trustee to exercise his discretion. The letter of wishes may be kept in a secure location and in various versions to cater for different requests to produce.

The protector

By appointing an accomplice as protector, the criminal may be maintaining a form of control over the assets even though he has lost legal title to them. This is of critical importance in a situation where the criminal believes the trustee is no longer doing his bidding or, as recent case law has shown, the trustee becomes suspicious and the authorities move to freeze the assets. The actions of a friendly protector in removing the incumbent trustee can be a valuable tool to hinder law enforcement agencies.

The type of trust

The trust itself will probably have an anonymous-sounding name and peculiar features that enhance its usefulness in a criminal enterprise. It may, for example, be a blind trust (a trust with no named beneficiaries) or it may purport to be a charitable trust. Such charitable trusts are often referred to as 'Red Cross Trusts' because the Red Cross, or a similar organisation, appears as the beneficiary in the trust deed. The charities, of course, never know about their interest and in most cases they are subsequently removed as beneficiaries in accordance with the true settlor's letter of wishes. This removal often occurs immediately before the payment of a distribution to the 'real' beneficiary who is often the settlor himself or another individual or entity under his control.

The use of companies

Often companies will be formed and their shares settled into the trust. Companies that are incorporated in jurisdictions with no disclosure requirement on identity details of beneficial owners to the authorities are attractive to criminals.

The provision of a registered office, corporate directors and nominee shareholders for companies that are ultimately owned by others is hugely attractive to criminals. If law

enforcement identify that such a company is connected with criminal property or to the commission of a predicate offence and they investigate, the hope will be that they will not identify the criminals connected with the company.

Companies are also vulnerable for the following reasons:

- Criminals can control companies without being officially connected to them through the use of corporate directors.
- Sizeable fluctuations in bank account activity appear less suspicious than on a personal account.
- Companies often have legitimate reasons for fund transfers between different jurisdictions and in different currencies.
- Some companies deal only in cash.
- Ownership of companies can be effected through the use of nominees or bearer shares without being officially connected to them.

Enhancing Vulnerability

The vulnerability of trust and company services is further enhanced through the delegation of control that is often given to clients and client advisers by company directors and trustees.

Such delegation of control comes in a variety of forms including:

- Powers of Attorney
- Bank signatories
- Representative offices
- Credit cards
- Distributions to third party non-beneficiaries

In addition, the culture of acquiescence evident in many trust and company service providers whereby client requests or directions are followed without question is pernicious. It is encouraged by the sheer volume of relationships that are required to be managed.

III. Case study

Whilst the theory of how gatekeepers operate is useful, a hypothetical case study based on facts which have had to be altered for the purposes of publication, illustrates how this may operate in practice. This may assist the reader in gaining a better insight into the mechanics.

The Chief Financial Officer (CFO) of a European manufacturing company wishes to benefit personally from contracts awarded by a government. Further, individual members of the government department commissioning the goods want to be rewarded for the award of the contract. The CFO already has an existing trust and company structure based in Switzerland for estate planning purposes. In order to provide legitimacy to the arrangements, the CFO advises his CSP in Switzerland that he requires a consultancy company which is to offer consulting services involved in the provision of 'strategic advice on negotiating contracts'. The CFO explains to the Swiss CSP that this is a natural extension to his activities for his employer, and negotiates an

attractive fee arrangement with the CSP based on a percentage of consultancy income. The company is incorporated in Panama and bearer shares issued to the CFO. He instructs a lawyer in Switzerland to draw up a consultancy agreement between the Panamanian company and the manufacturing company. Further, the individual members of the government department are to act as consultants to the Panamanian company and remunerated on the basis of performance criteria to be determined by the CFO. They do so through separate 'employment' or 'agency' companies that enter into contracts with the Panamanian company for the supply of services to it. The Swiss lawyer is also involved in drawing up *pro forma* consultancy agreements.

The CSP receives money into a designated account in the name of the company that has entered into the agreement, from the government department and pays invoices submitted to it by the 'consultants' for services rendered under the various consultancy agreements. The CFO submits invoices for his services and requests that these sums are paid into the pooled account of a Jersey CSP which administers a discretionary trust established for the benefit of his children. The 'real' beneficiaries have not yet been added to the trust instrument due to reasons of 'confidentiality'. The CFO advises the Jersey CSP that these funds represent performance bonuses related to consultancy services, and provides a copy of the consultancy contract. As settlor of the trust and under a Letter of Wishes, he requests that these funds be conservatively invested in a portfolio of blue chip stocks.

1. Case study analysis

At each stage of the above case study it can be seen that gatekeepers, in the form of the following:

- Swiss CSP establishing the Panamanian company issuing bearer shares
- Panamanian incorporation agents
- Lawyer involved in the drawing up of the consultancy agreements between the Panamanian company and the government department, and the Panamanian company and the consultants
- Bankers' provision of a pooled account, thereby making identification of the funds more problematic
- Jersey CSP administering the discretionary trust under a Letter of Wishes with unnamed beneficiaries

have each facilitated the laundering of the proceeds of crime. Although in the above example, there is no one individual gatekeeper masterminding the operation, by separating out each of the stages of the process, the criminal has been able to fragment the overall picture. As a result, each gatekeeper is placing some form of (unwarranted) reliance on another party or documentary evidence provided by another party to derive comfort as to the *bona fides* of the transaction. At no stage do any of the gatekeepers seek to test, beyond what they are told or are presented with, the rationale of the transactions.

The authors' views are that this is often a function of either greed, incompetence or a reluctance to verify the information being provided for fear of losing a lucrative client. As discussed above, there are also gatekeepers who intentionally provide services to criminals and are knowingly complicit in their crimes. These gatekeepers are often the most difficult to detect as they are usually familiar with circumventing the anti-money laundering defences of most financial institutions and are aware of the 'soft spots' where vulnerability is the greatest. Having established strong relationships with financial institutions, these gatekeepers will continue to exploit any perceived loophole and, critically, play on the human relationships established in order to be able to either

override controls or to influence individuals to exercise their discretion in such a way as to benefit their client.

In the authors' experience 'birds of a feather flock together'. The same gatekeepers frequently appear in cases of laundering abuse. Once a reputation for weak standards of due diligence and a culture of acquiescence to client demands is established, word spreads quickly throughout the criminal fraternity.

IV. Conclusions

The vast majority of gatekeepers whether they be lawyers, accountants, corporate services providers or trustees are perfectly legitimate. Most of their clients use their services and buy their products for lawful reasons. However, the features that make many of those products and services attractive to legitimate consumers also make them attractive to criminals.

As the Financial Action Task Force (FATF) has noted, there is an increased use of 'legal persons' as opposed to natural persons, coupled with the increased use of professionals to provide assistance in laundering criminal funds. However, despite FATF Recommendation 12, which stipulates that designated non-financial businesses and professions (DNFBPs) should apply the customer due diligence and record keeping requirements as promulgated by FATF, there continue to be weaknesses that criminals easily exploit.

Critically, the effort to strengthen the defences of gatekeepers must be global. Money laundering and terrorist financing are a global problem. They demand a global solution. Differences in domestic anti-money laundering (AML) rules as they apply to trustees, lawyers and so on undermine the global effort. The difference in approach to tax evasion between the United States and Switzerland brought into sharp focus by the recent UBS case illustrates the point. Inconsistencies provide opportunities that are often readily exploited.

Lawyers and accountants are a very powerful lobby group. Despite that, many countries have successfully implemented legislation to bring the professions into the net of AML regulation. Now it is incumbent upon those countries to demonstrate the political will to enforce the rules against professionals unhesitatingly. Until then, gatekeepers will continue to be a weak link in the AML and counter-terrorist financing chain.

KEITH OLIVER*

Civil interim measures in England**

I. Introduction

This chapter gives a practical overview of key civil interim measures and remedies available from the English civil court for securing recoveries for a victim of fraud, corruption or other acquisitive crime. The remedies described are regarded as the lawyers' 'Nuclear Weapons' and are often known as such. Properly applied for and used, freezing property and search orders can put the claimant in the strongest possible position on day one of the proceedings to trace, secure and recover the proceeds of the claim or fraud or corruption upon him, however that crime has been perpetrated. Dishonest defendants or those whose conduct requires it find they are suddenly – and without advance warning – hamstrung financially and may in practical terms be deprived of the oxygen of financial resources to go about their daily lives. With the surprise elements of a pre-emptive strike by way of freezing order and ancillary asset disclosure and tracing orders, the defendant often suffers a mortal wound to his defence from which there is no ultimate recovery to avoid judgment and execution of that judgment worldwide. For the purposes of clarity throughout the chapter C refers to the claimant victim(s) of the fraud or corruption, D refers to the defendant perpetrator(s) and T refers to third party accomplices.

To secure recovery it is necessary to have sufficient evidence to bring valid claims against D and sufficient assets against which a judgment can be enforced. Victims of fraud and corruption will be minded to (i) preserve assets to satisfy the expected civil judgment against D; (ii) preserve evidence that D might destroy or withhold if he becomes aware that the criminal offence has been discovered; (iii) obtain evidence from third parties that will aid the intended civil claim. Interim measures discussed below help achieve these objectives.

The following three sections consider freezing (Mareva) orders, proprietary injunctions and other key ancillary orders. The fifth section focuses on search (Anton Piller) orders and the sixth examines other relevant considerations namely, illegally obtained evidence and the privilege against self-incrimination.

* Keith Oliver is a Senior Partner at Peters & Peters and heads the firm's specialist Commercial Litigation/Civil Fraud and Asset Tracing Team. He specialises in international and domestic civil and commercial fraud litigation, asset tracing/ recovery, regulatory, insolvency and trust litigation.

** This chapter is not intended to be a substitute for legal advice or a legal opinion. It deals in broad terms only and is intended to merely provide a brief overview and give general information.

II. Freezing orders

1. Background

The order takes its name from *Mareva Compania Naviera S.A. v International Bulkcarriers S.A.* [1975] 2 Lloyd's Rep. 509. The Civil Procedure Rules now refer to it as a freezing injunction (CPR 25.1(1)(f)).

It developed as a form of recourse against foreign-based defendants with assets within the UK and consequently the early authorities assumed that the injunction was not available against English-based defendants. In the same vein an early judicial guideline for the grant of the order required claimants to establish a risk of the removal of assets from the jurisdiction.

Section 37(3) of the Supreme Court Act 1981 now provides that the injunction may be granted to prevent defendants from removing from the jurisdiction 'or otherwise dealing with' the assets. Section 37 forms the basis of the jurisdiction for granting freezing injunctions 'in all cases in which it appears to the court to be just and convenient to do so'. The Court of Appeal held in *Babanaft International Co. S.A. v Bassatne* [1990] Ch. 13 that the wording of subsection 3 did not restrict the scope, geographical or otherwise, of s.37(1). The Civil Procedure Rules currently provide that the injunction may be granted in relation to assets 'whether located within the jurisdiction or not' (CPR 25.1(1)(f)).

2. Purpose and effect

A freezing order prohibits D from unjustifiably dissipating his assets within the jurisdiction so that there are insufficient or no assets left to satisfy a judgment against him. To preserve assets pending enforcement, a freezing order can also be obtained post-judgment. If D has insufficient assets within the jurisdiction to meet the quantum of C's claim, the court can grant a worldwide freezing order.

3. Penal notice

Freezing orders, as well as search orders, are endorsed with a Penal Notice, which warns that disobedience of it may be regarded as contempt of court the penalty for which may be imprisonment, a fine or seizure of assets. Contempt may extend to any third parties who are notified of the order and do anything which helps or permits a breach its terms. However since the English court has no jurisdiction over third parties located abroad, the worldwide order has to be recognised, registered or enforced by the relevant foreign courts to be effective. This process is often described as 'domesticating' the English order.

The orders usually freeze assets up to a financial limit, calculated according the value of C's claim with likely legal costs and interest taken in to account. D can deal with any '*surplus*' assets that exceed the limit of the order as he sees fit. In addition payment of a sum equal to the value of the limit into court or providing security in that sum can discharge the freezing order.

A freezing order bites on the individual not his assets (*in personam*) and as such it does not grant any proprietary rights over the assets of D. It therefore does not confer on C any advantage in the event of D's insolvency. However, the position is different where proprietary rights are claimed over frozen assets (see Proprietary Injunctions below). A freezing order is an interim measure and therefore the standard form of order permits D to draw on frozen assets to pay a '*reasonable sum*' for legal expenses

and to pay a pre-set sum (fixed by the court) to meet ordinary living expenses. C is given a measure of control over any increases in expenses in order to prevent D from depleting his assets improperly. For example any increase in expenses has to be agreed with C, or in the absence of agreement, approved by the court.

4. Asset disclosure

The standard freezing order requires D to give details of the value, location and details of assets within the jurisdiction or elsewhere, for a worldwide freezing order. This enables C to identify the whereabouts of the assets and notify third parties of the freezing order. D may refuse to provide some or all of this information if in providing it, he is likely to incriminate himself. The assertion of self incrimination privilege has been much curtailed in the United Kingdom (UK) by the Fraud Act 2006 – and in practical terms by the fact that reliance on the privilege is generally regarded as in effect an admission of liability. Forcing the fraudster defendant into an assertion of self incrimination privilege can be the first stage in victory for the claimant victim. Where there are concerns about the completeness of D's disclosure on affidavit, C can apply to have D cross examined in relation to those assets. In addition, the court can grant orders requiring third parties (e.g., banks) to assist in identifying and locating assets and other relevant information.

5. Application and requirements

The application to the court for a freezing order, as well as a search order, is almost invariably made *without notice* to D (*ex parte*). The first time that D learns about the order should be when he is personally served with it (see below for more detail about Service). This is done so as not to '*tip off*' D and T about C's intention to commence proceedings or to take any legal steps to secure assets and/or evidence. The court may decide not to grant a freezing order if D has had notice of C's intentions because '*the court is unlikely to make orders which are futile*' (*Oaktree Financial Services v Higham* [2004] EWHC 2098 Ch [10]).

6. Grounds

In order to obtain a freezing order, C needs to show:

- A good arguable case; and
- A real risk of unjustifiable dissipation of assets; and
- That the order is just and convenient in all the circumstances

The court will not automatically conclude that because D is alleged to be dishonest he cannot be trusted not to dissipate his assets. Careful consideration should therefore be given in the evidence to the profile and background of D.

7. Cross-undertaking in damages

The court will require C to give a 'cross-undertaking in damages' which is a promise to comply with any order that it may make if it decides that the freezing order caused loss to D and that D should be compensated for that loss. This may include provision of security to fortify the cross-undertaking in damages.

8. Full and frank disclosure

On a *without notice* application the court is being asked to grant a hugely intrusive order against D who has not had a chance to be heard. Therefore C and his lawyers must give full and fair disclosure of all the material facts, including what D is likely to argue in his defence, or against C, or any facts likely to be relied upon. If there has not been full and frank disclosure, there is a real risk that the court will set aside the order.

9. Service

Personal service is usually a precondition to committal for contempt of court for a breach of an order endorsed with a penal notice. However, the court does have an inherent discretion to vary the requirements for personal service (RSC Order 45.7(7)). Where relevant and possible, service should be effected simultaneously on D and the third party asset holders.

III. Proprietary injunctions

If C contends that D is holding C's property (which can include cash) or the traceable proceeds of his property (the '*proprietary assets*') then the court can grant a proprietary freezing injunction. Its terms are typically more draconian than a standard (non-proprietary) freezing order and can restrain any dealings with the proprietary assets so that D cannot use them to pay for living or legal expenses.

When applying for a proprietary injunction, C needs to show a good arguable case and that it is just and convenient that the order be granted. He does not need to establish a risk of dissipation, because the nature of C's claim is that D is holding his assets or the proceeds of those assets. As a result the proprietary injunction does give C priority over D's creditors on the asset pool.

IV. Ancillary orders

The English courts have developed a number of orders to assist victims of fraud and corruption in their fight against those who attempt to delay and obfuscate. These include specific disclosure orders, which require disclosure of particular documents to help identify the nature and location of assets or passport orders requiring delivery up of all travel documents and prohibiting D from leaving the jurisdiction. A fraudster[1] suddenly deprived of the means of travel internationally is inevitably shocked by the severity of the civil court's powers and it immediately impacts particularly if he is an overseas national who cannot return home or leave the UK during the currency of the asset disclosure process. Third party disclosure (*Norwich Pharmacal*) orders require third parties who are mixed up in the wrongdoing (whether innocently or not) to disclose information that will assist in the identification of wrongdoers, allow assets to be traced and to establish the validity of proprietary claims against third parties or

1 In this context a fraudster denotes a person who may have committed criminal offences but who, for the purposes of this chapter, is the subject of the full panoply of civil measures that are available in the UK and also possibly in other jurisdictions.

tracing assets into the hands of third parties. Banks through which stolen funds are believed to have passed are an obvious target for such orders.

In addition third party freezing orders can be obtained against third parties but only where there is good reason for believing that assets ostensibly held by third parties are in reality D's assets. This is known as the *Chabra* jurisdiction. These orders are particularly useful where D has structured his affairs through sham trusts or other opaque vehicles so as to give the impression that he has no interest in the assets in question.

A critical weapon for the claimants is to be found in section 25 of the Civil Jurisdiction and Judgments Act 1982. Section 25 allows an English court to grant interim relief in aid of proceedings elsewhere. These are commonly invoked where assets are located in England, but D is located outside the jurisdiction, in the place where the substantive proceedings are being conducted. It is not necessary for foreign proceedings to have been commenced as long as they will be commenced. One can obtain relief in England – subject to demonstrating a sufficient geographical nexus – which cannot be obtained in the location of the substantive action.

V. Search orders

1. Purpose and effect

Search orders are directed towards preserving evidence which D would otherwise destroy or suppress if he learnt of C's intention to take legal action against him. The order requires D to permit access to C's solicitors to his '*premises*' to search for and seize specified evidence.

The order does not allow forced entry. It imposes an obligation on D to permit entry to his premises. A failure or refusal to grant access will be contempt of court punishable by imprisonment and/or a fine. Search orders are by their nature intrusive and psychologically destroying to the defendants, particularly as standard form orders do not limit the extent of the search and permit the electronic imaging of computers, mobile phones, PDAs and Blackberries to secure information, normally defined by reference to the substantive allegations as the case study that follows this chapter neatly shows.

2. Application and requirements

As with freezing orders, search orders are made without notice. Therefore, C has to provide a cross-undertaking in damages and comply with the full and frank disclosure obligation. The order is also endorsed with a penal notice and contempt may extend to any third parties who are notified of the order and do anything which helps or permits a breach its terms.

The following conditions must be fulfilled in order for the claimant to obtain a search order:

- There must be an extremely strong *prima facie* case
- Evidence of very serious potential or actual harm to the claimant's interests
- Clear evidence that D possesses the relevant incriminating evidence
- That there is a real possibility that D will destroy the material before an inter-partes application can be heard

- The harm likely to be caused to D and his business affairs as a result of execution of the search order must not be excessive or out of proportion to the legitimate object of the order
- In addition, the court must also be satisfied that the order is just and convenient in all the circumstances

The court requires that an independent solicitor is appointed (known as the supervising solicitor) to serve the order on D and also oversee its execution to ensure that it is conducted fairly.

D is permitted to arrange legal representation and also to gather up any documents he believes are legally privileged or which may incriminate him and hand those documents over to the supervising solicitor. If the supervising solicitor determines that the documents may be incriminating or privileged, or is in any doubt as to their status, then he will exclude them from the search and retain them in his safe custody, pending further order of the court.

No one who might gain commercially or personally from what they may see in the course of execution of the search order is permitted to execute the order. This typically means that C is not permitted to attend. C's legal representatives will execute the order.

VI. Other relevant considerations

1. Illegally obtained evidence

Great care should be exercised to ensure that information obtained in the course of the investigation has been obtained lawfully. Examples of illegal sources of information include dishonest pre-text calls, information obtained in breach of data protection laws and hacking. Illegally obtained evidence is admissible before the civil court but the court will decide how much weight to attach to the information and also it will consider whether to exercise its discretion and make the order sought given the provenance of the evidence.

Illegally obtained evidence is disclosable. The general rule is that evidence obtained for intended litigation normally attracts legal professional privilege. This means that the existence of the investigative materials and work product has to be disclosed but the documentation and work product itself is privileged from production and inspection (i.e., D is not allowed to see it).

However, there are exceptions to this rule: in *Dubai Aluminium Co Limited v Al Awi and Others* [1999] 1 WLR 1964 the judge held that where criminal and fraudulent conduct was involved for the purposes of acquiring evidence in or for litigation, any documents generated by or reporting on such conduct and which were relevant to the issues in the case were not only disclosable but also were not protected by legal professional privilege and therefore could be inspected by the other party. If evidence is obtained illegally and this is not disclosed to the court, in accordance with the obligation of full and frank disclosure, then if D learns about it, he may attempt to apply to discharge the order that was obtained *without notice* with the benefit of that evidence on the basis of non-disclosure and also argue that the order should not be renewed at the *inter-partes* stage.

VII. Privilege against self-incrimination

Freezing, proprietary and search orders contain mandatory provisions requiring the provision of specific information. The orders contain exceptions so that D may refuse to provide information or documents on the grounds that to do so would incriminate him.

The starting point is section 14(1) of the Civil Evidence Act 1968 which provides that the defendant may refuse to answer any question or produce any documents or things if to do so would tend to expose that person to proceedings for an offence or penalty.

However, section 13 of the Fraud Act 2006 has had a dramatic effect on the privilege against self-incrimination. It came into force on 15 January 2007 and, because it is simply an evidential provision, it applies retrospectively. It provides that a person is not to be excused from answering any question put to him in proceedings relating to property or complying with any order made in proceedings relating to property on the ground that doing so may incriminate him or his spouse or civil partner of an offence under this Act or related offence. A statement or admission made by a person in answering such a question, or complying with such an order, is not admissible in evidence against him or his spouse or civil partner in proceedings for an offence under this Act or a related offence.

Under the Act '*proceedings relating to property'* means any proceedings for the recovery or administration of any property; the execution of a trust and an account of any property or dealings with property. Property covers any money or other property whether real or personal, including things in action and other intangible property. Related offence means conspiracy to defraud and any other offence involving any form of fraudulent conduct or purpose. In *Kensington International Limited v Republic of Congo* [2008] 1 Lloyd's Rep. 161 it was held to include bribery.

VIII. Conclusion

The international nature of fraud, corruption and indeed any acquisitive offence involves asset transfers across territorial borders. Careful thought to the choice of jurisdiction and the possible or actual civil, criminal or regulatory processes in those jurisdictions and their effect on the civil recovery strategy are value judgments that must be made with the benefit of the fullest possible information and long term strategic aims in mind. Invariably foreign (local) specialists play an essential role in the international asset tracing and preservation exercise but the team must be cohesive, focused and instantly connected without egocentric national perspectives. Pursuing such criminals is a worldwide exercise where all the relevant jurisdictions have an equally important role to play. Properly managed and directed, the recovery of stolen or corruptly acquired assets through the panoply of civil remedies available can be expeditious, cost effective and devastating for the criminals as the following case studies demonstrate.

Case studies

1. The Banco Noroeste story – the investigation, tracing and recovery of USD 242 million stolen from the Bank in an elaborate multinational '419' advance fee scam

The use of multinational litigation and, particularly, the combined application of civil and criminal processes working in parallel as part of a litigation pincer movement produced extraordinary successes in the recovery of the millions looted from Banco Noroeste of San Paolo, Brazil in the late 1990s – even though the recovery litigation did not start until several years later.

The head of the international division of Banco Noroeste of Brazil, Nelson Sakaguchi (Mr Sakaguchi), stole USD 190 million from the Bank through falsification of cash balances it held offshore in the Cayman Islands in a fraud of breathtaking audacity. Nigerian 419 fraudsters duped Mr Sakaguchi into believing that they were Nigerian government officials charged with the construction of the new international airport in the Nigerian capital of Abuja. The black hole was discovered in 1998 as part of the due diligence process for the impending sale by the majority shareholders of the Bank of their controlling interest to Banco Santander. By then the proceeds of the fraud – amounting to USD 242.5 million inclusive of interest and costs – had been laundered throughout the world.

The laundry extended to Hong Kong, Switzerland, UK, the United States (US), Singapore and ultimately Nigeria. The funds had been misapplied through SWIFT transfers – from the US to a multiplicity of accounts worldwide for the ultimate benefit of the key fraudsters, primarily Nigerian nationals by name of Emmanuel Odinigwe Nwude (Mr Nwude) and the late Christian Anajemba (Mr Anajemba) and his widow, Amaka, through a currency exchange laundry. The laundering had been managed initially through Hong Kong and subsequently Switzerland by Shamdas and Naresh Asnani (Asnanis), who were importers and exporters of electronic equipment between Hong Kong and Nigeria. It was the Asnanis who dishonestly secured the use of private Swiss bank accounts through which no less than USD 122 million was laundered as part of, purportedly, a black market foreign exchange operation that involved the trading of stolen dollars for Nigerian Niara.

Key to the successful recovery was the inclusive approach adopted by the multinational legal team involving eight jurisdictions with simultaneous proceedings. Aside from civil proceedings in the UK, the US and Hong Kong, simultaneous civil and criminal investigations and proceedings were commenced in Switzerland and subsequently in Nigeria. The criminal investigation in Switzerland secured the freezing of key bank accounts identified through the forensic determination of the fund flows. Simultaneous disclosure proceedings in the UK were directed at various banks through which funds had been channelled – key to the disclosure process (see section IV, first paragraph) are the gagging provisions of the disclosure order mechanism so that the banks innocently caught up in the channelling of misappropriated funds are prevented by Court order from disclosing the fact of disclosure, i.e., of the proprietary information they hold, to the owners of the account(s).

The Swiss legal team acting for the Banco Noroeste claimants (in Switzerland the *Parties Civiles*) were afforded early access to the information generated as part of the criminal investigation in Geneva. A picture fast emerged of a world wide web of illicit transfers involving the acquisition of valuable real estate in London by the Anajembas and in California by Mr Nwude and members of his immediate family and purported business activities by the Anajembas in Kentucky. Pursuant to a warrant issued by the *Juge d'Instruction* in Geneva, Mr Sakaguchi was arrested in New York and transferred

to stand trial, following lengthy incarceration, in Geneva. His co-defendants were the Asnanis who were similarly arrested in Miami pursuant to arrest warrants issued in Switzerland. Their lies to Citibank and Lloyds TSB International in Geneva and Zurich regarding the ownership of the funds remitted to the banks were serious breaches of Swiss banking law. They were money launderers. Information they provided both as part of the examination process – undertaken in the presence of the recovery team's lawyers – was applied worldwide. Mr Sakaguchi and Narash Asnani were convicted and spent over two years in a Swiss jail. Their conviction of Swiss money laundering offences demonstrates that overseas nationality is no bar to the full force of domestic law where international fraud is concerned.

In the UK interim and summary judgment against Amaka Anajemba both on her own account and as the widow and key beneficiary of her assassinated husband's estate for, respectively, USD 150 million and USD 290 million was secured as was judgment against one of the smaller players Chief Ezuge Nwandu (Mr Nwandu). It was Mr Nwandu's GBP 100 company, MacDaniels Limited, that effected the laundering of USD 8 million through the East London branch of a UK clearing bank, key transactions in the tracing process which enabled London to act as the spring-board jurisdiction for the worldwide civil litigation. The civil judgments against Amaka Anajemba and subsequently Mr Nwude were transported to Nigeria and California respectively. The US legal team secured judgments against Mr Nwude in California which were similarly spring-boarded to Nigeria. The UK proceedings alone involved 42 defendants and the range of asset tracing weaponry such as search and seizure orders, freezing orders, passport orders, *Norwich Pharmacal* orders (disclosure orders), interim payment orders, summary judgment, third party debt orders, charging orders and orders for sale. The UK legal team discovered that the late Mr Anajemba had acquired prior to his death extensive residential investment property in North London and extraordinarily had continued despite his death to pay tax on the rental income as part of the continued fiction.

Until the Banco Noroeste case, it had long been thought that recovery of stolen assets by proceedings in Nigeria was a near impossible task. The successes secured by the Banco Noroeste legal team working in conjunction with the EFCC – the Economic and Financial Crimes Commission established by the Nigerian Government to tackle money laundering offences head on – were spectacular. In July 2005, Amaka Anajemba pleaded guilty following a plea bargain arrangement and an agreement with the Banco Noroeste complainants. She received a 30 month sentence, fines of USD 5 million and N 1 million. In addition, assets worth USD 20.25 million were forwarded to the complainants, this aside from the civil recoveries already made against her and her deceased husband both in London and in Kentucky. In November 2005, Mr Nwude and another conspirator Nzeribe Okoli pleaded guilty receiving respectively five and four year sentences and orders to forfeit assets. The recovery process remains ongoing – over USD 120 million has already been recovered in cash, property and inevitably perhaps the fleet of expensive luxury cars.

Key to the legal operation and the successful recoveries was a number of central factors. The victim claimants' determination to pursue the launderers despite what might have appeared to be insuperable legal odds; the application of the initial recoveries to fund the litigation worldwide so that it was cost effective. The combined use of the civil and criminal jurisdictions – civil in the common law countries such as Hong Kong, UK, the US and Nigeria – and the combined criminal and civil mechanisms in the civil law jurisdiction of Switzerland with the ultimate application of the successful remedies by jail sentences both there and in Nigeria. The flow of monies internationally and the recovery and tracing steps available through the courts shows that there are in the modern world very few places that the fraudster or perhaps corrupt government official banker or ex-politician can ultimately hide.

2. The Brian White story

The Brian White Story – and the claims made against him by the Russian businessman that he conned – raises important issues concerning freezing orders, passport orders and the jurisdiction of the UK Court to issue a civil bench warrant to enforce a freezing order.

Mr Brian White (Mr White) had acted as agent for companies and property interests owned by a leading Russian businessman, Oleg Zakharov (Mr Zakharov), in connection with various investments and financial transactions including a major property development near Sotogrande in southern Spain. Mr Zakharov claimed that Mr White had failed to act honestly in relation to funds transferred to him and into accounts under his control and had dishonestly misappropriated assets and money belonging to him including shares and offshore companies primarily in the Dutch Antilles. Mr Zakharov made proprietary claims for the return of his property and that of his companies together with claims for compensation and damages for breach of fiduciary duty, conversion and breach of contract. The claims ran into several million Euros.

Mr White was elusive and difficult to trace. He was ostensibly located in Gibraltar and southern Spain but operated an accommodation address in Surrey, England, from where he used to direct his post using the confidential postal box system. Following detailed investigative work and an extensive forensic examination of the fund flows between Mr Zakharov's companies and the vehicles controlled or operated by Mr White, Mr Zakharov made application for worldwide freezing order relief including a passport order requiring Mr White to immediately deliver up his passport and other travel documents and a prohibition upon him travelling outside the jurisdiction of the Court.

When confronted with the freezing order requiring him to deliver up his passport and the key documents relating to the subject matter of the proceedings, Mr White refused to cooperate in any way. He claimed that his passport was held by an elderly relative in Scotland and notwithstanding the clearest possible warning that failure to comply would lead to contempt of proceedings his reaction was one of flagrant disregard for the Court order.

He took possession of the case papers and sped off in his vehicle into the Surrey countryside. Fearing that he was about to flee the jurisdiction, Mr Zakharov's lawyers followed Mr White but in the ensuing chase, he managed to lose them. However and simultaneously, Mr Zakharov's lawyers were able to make immediate urgency application to the Judge who made the original freezing and passport order, coordinating that process remotely enabling an application that afternoon to be made for the issue of a bench warrant for Mr White's arrest.

Mr White, within a matter of hours, was arrested at the mansion he occupied with his partner and which had been acquired using funds misappropriated from Mr Zakharov through the mechanism of a Dutch Antilles' entity which was one of the key vehicles of the fraud that Mr White had perpetrated.

Mr White's conduct in the face of the order and his clear disregard for the obligations imposed upon him by the Court led within a matter of months to a bankruptcy order against him and judgment with full recovery by Mr Zakharov of the property and cash assets both in the UK and Spain that Mr White had misappropriated.

The case demonstrates the immediacy of the freezing order regime and how this, allied to the weaponry available to the civil asset tracing legal team, can produce spectacular results for the victim claimant. Mr White – unversed in international litigation of this kind – never imagined the full force of English law would operate so as to compel the

delivery up of his passport, the immediate disclosure of his worldwide assets and an order obliging him to co-operate with the tracing and recovery of assets which at that stage it was alleged that he had misappropriated. The without notice (*ex parte*) effect of the asset tracing civil law weaponry is an extraordinary jurisdiction and one which the victim claimant should employ whenever the evidence justifies it. The assets disgorged by Mr White included, aside from the property cash assets, the valuable executive toys so beloved of fraudsters, in this case the proceeds of a helicopter and a top of the range Aston Martin!

3. General

As technology advances daily, the English Courts have shown themselves, time and again, to be adept and creative in assisting the victim claimant to recover the proceeds of fraud and corruption. The last years have seen an explosion of applications made under Section 25 Civil Jurisdiction and Judgment Acts (see section IV, last paragraph) – this enables the Courts on application without notice by the victim to utilise the panoply of weaponry available to the Court to assist a foreigner with jurisdiction in its pursuit of the fraudster or corrupt official. The dictator, the businessman, the ex-politician or the 419 crook against whom proceedings have been started or are about to be started in a host domestic state – wherever in the world that may be – can find themselves the subject of International Freezing and Tracing Order relief where proceedings are commenced in England on the basis that there is sufficient nexus with England and Wales to justify it. The nexus can be in terms of the location of property, perhaps a small shareholding in an operating company in which the defendant has a claimed beneficial interest, even if owned offshore but beneficially by him, or by the simple expedient of him being present in England and Wales at a particular time so that service upon him, *in personam*, can be effected.

The Section 25 jurisdiction is far reaching and often causes amazement to those unaware of its implications – witness for example a defendant with no apparent connection with England who is served with a freezing order requiring the worldwide disclosure of his assets issued by an English Court in ancillary support of proceedings in an European Union country relating to his alleged breach of duty while the director of an international conglomerate. Failure to make worldwide disclosure of his assets to an English Court, even though the subject matter of the fraud or corruption arose in a different jurisdiction, represents a contempt of Court punishable by imprisonment or segregation of assets. This where the subject matter of the alleged fraud or corruption has nothing whatsoever to do with England. The jurisdiction is secured by the expedience of property or *in personam* jurisdiction.

Technological advance in future years will doubtless enable the Courts to devise orders directed at the recovery of proprietary information held by internet servers providers and mobile phone operators (so that SMS messages can be retrieved aside from e-mail). Aside from the fund flows through the banking systems, developments of this kind enable the claimant lawyer to steal yet another march on the misapplication of laundered funds by the criminal – and this a civil process, though one that co-exists and operates very effectively as we have seen in the Banco Noroeste case with a parallel criminal investigation, prosecution and jail for the wrongdoer.

MARTIN KORTE* AND CHRISTIAN MUTH**

The involvement of private investigators in asset tracing investigations

I. Introduction

Asset tracing investigations have become an important tool in international business as both economic uncertainty and the unreliability of information have increased significantly. The increasing complexity of the global financial system adds to the importance of asset tracing, especially with the introduction of sophisticated financial instruments and integrated business activities. Within this framework, corrupt public officials, fraudsters and others are able to realise their criminal intentions far more easily as the flow of stolen funds and assets can be almost perfectly concealed from detection.

Against this background, asset tracing can be successfully applied in various ways, either *ex ante*:

- Locating and evaluating underlying assets before entering into equity and credit deals, e.g., loan collaterals
- Tracing assets prior to bankruptcy to determine title to assets

or *ex post*:

- Whenever assets have been embezzled, stolen or misappropriated by sophisticated fraudsters or rogue state leaders in which case asset tracing may lead to criminal or civil proceedings (i.e., arbitration, litigation)

In criminal matters, the asset tracing investigation is generally followed by an asset repatriation process during which the stolen assets are seized and repatriated after legal proceedings.

Private investigators play an increasingly important role in tracking stolen assets. The following chapter takes a look at the current state of affairs and challenges in order to successfully manage asset tracing investigations.

II. Core competencies for private investigators in asset tracing

The requirements for conducting successful asset tracing investigations are high, as are the stakes for the participating parties. This is due to several factors:

* Martin Korte is a Senior Consultant with the Ernst & Young Fraud Investigation and Dispute Service Department based in Frankfurt, Germany.
** Christian Muth is a Senior Consultant with the Ernst & Young Fraud Investigation and Dispute Service Department based in Frankfurt, Germany.

- Assets usually do not remain in the same location but are transferred to off-shore or other 'exotic' countries
- Evidence of assets are concealed in complex financial transactions or accounting records
- Movement of assets between countries results in the need to understand the different legal requirements for asset tracing investigations in each country

Accordingly, the range of potential players in the asset tracing arena is rather narrow.

First, an investigator must have the necessary legal background to be able to establish who has the legal title to the assets that are to be tracked.

Second, the investigator also needs to have excellent accounting skills as smart operating fraudsters and corrupt officials try to hide their tracks through complex accounting and financial transactions. Today's complex global financial system complicates the detection of stolen assets significantly, requiring the investigator to know about current developments and innovations in the financial sector to be able to understand complex transactions and instruments and how they can be used to hide funds and assets.

Most importantly, a successful investigator needs to be able to rely on an international network of business partners and affiliates located in multiple countries to ensure a thorough understanding of the local laws and regulations with regard to asset tracing. This network can also help in conducting business partner screening and even taking on the asset tracing investigation once a clear link to the respective foreign country has been established.

Not all private investigators necessarily meet the requirements described above. Internationally active companies in the security and intelligence sector are at an advantage, for example, simply because of their wide ranging network of subsidiaries and affiliated companies in other countries.

For the same reason, large professional services firms have also taken on the task of tracking down assets by introducing special units that are usually part of their forensic services department. Such departments are often composed of interdisciplinary teams with different backgrounds such as law, accounting, Information Technology (IT), law enforcement and intelligence. Because knowledge and background are shared in such teams, investigations can be conducted more effectively and efficiently based on this alignment of know-how. Beyond the interdisciplinary focus, most investigation teams also offer specialisation based on different industries, as these often display different characteristics in terms of what kind of assets and how these assets are misappropriated (e.g., banking industry vs. technology sector).

III. Conducting asset tracing investigations

Asset tracing investigations generally require a focused and consistent approach in order to achieve their ultimate objective: identify assets underlying a business deal or recover assets that were misappropriated.

However, asset tracing cannot be conducted according to a pre-designed checklist as there are too many unknowns and different factors that can influence the direction of the investigation. Nonetheless, there is one requirement that needs to be adhered to for all asset tracing investigations: document the findings. As there is always the potential for future legal proceedings (or such proceedings may, in fact, be the cause of an investigation), the requirements for documenting the actions taken, procedures

performed and outcomes are high. For example, expert interviews with witnesses have to be transcribed and searches of electronic files and databases recorded in order to have solid ground for admissibility in court, including evidence that the information gathered was legally acquired and is verifiable.

The following sections describe an approach for successfully conducting an asset tracing investigation, in order to be in a position to identify suspicious transactions that can provide the final lead to the stolen assets.

1. Know the parties involved

Identifying the individuals and companies involved in an asset misappropriation scheme is the first step of any asset tracing investigation, aimed at gaining an overview of what private and professional relationships exist between the parties involved. Furthermore, it may provide insight into the financial and proprietary conditions of, for example, a potential business partner. As not all the parties involved are known from the outset of an investigation and may only become apparent in the course of an investigation, (e.g., after reviewing contracts, namely, who are the parties to a contract, and other documents, analysing financial transactions, namely, who is the beneficiary of a financial transaction), the gathering of intelligence on parties involved is an ongoing part of an investigation. The research for intelligence on the parties involved takes place in public registers and databases, such as commercial registers, court filings, rating agencies, business databases, phone books, asset registers etc. At times, simple Internet research can lead to extraordinary results. However, if no information is available through these sources, the required information can be captured by on-site inspections and conducting interviews with third parties, e.g., business partners, witnesses, creditors and other stakeholders, as will be discussed in further detail later.

The outcome of the intelligence gathering process should be somewhat called 'the big picture' where all the different leads to the parties involved are included. But how does an investigator paint 'the big picture' in order to convey it to other parties, to make it visible?

Investigators use software specifically designed for illustrating personal and professional links between individuals and companies involved in asset misappropriation schemes. The basis for establishing the links is the information acquired during the intelligence gathering process. Myriads of pieces of information, such as names of individuals and companies, addresses, phone numbers, birthdates, Internet domains, bank account data etc., are put together in a flowchart. The software automatically links the pieces of information and creates a 'data web.' This data web can be used to conduct a link analysis in order to determine the title of assets or to identify cross links between different entities and individuals. For example, a link analysis may identify the holder of a bank account who was not the focus of the investigation but who, by acting as a middleman, played an important role in the transfer of funds to off-shore bank accounts. Or the ownership of a consulting company that received a large amount of cash for providing 'fictitious' services may become visible only after the pieces of the intelligence puzzle are put together in a data web.

In order to gain an understanding of the financial background of a potential business partner, solid intelligence gathering and the visualisation of its results in link-analytical charts is crucial to a successful asset tracing investigation.

2. Analyse electronic files and databases

The analysis of electronic data, such as e-mail accounts, files, phone registers and other databases is another important step in obtaining information on the destination to which assets or funds may have been transferred. Proper performance of this step is critical due to strict privacy laws in some countries, requiring the investigator to be aware of the legal consequences that may accompany the data analysis. Obtaining access to the data itself often frustrates performance of this step, as described in greater detail later.

Based on the results of the intelligence gathering process, the investigator should have formed an initial idea on the individuals and entities for which to search within the electronic data. The search criteria for conducting the electronic file analysis do not only include basic data such as the names of the individuals and entities but also other terms such as account numbers, addresses, dates, phrases, description of assets and other objects etc. The key word searches can be performed based on a variety of e-discovery tools such as Attenex, Nuix, Introspect, dtSearch and others.

While the basic intelligence gathered may show links between individuals and entities based on mostly publicly available information, the analysis of electronic file data provides insight into the interactions between the individuals, either representing themselves or the entities. Also, compared to the process of conducting interviews, the results of the data analytics process are actually in a written format and thus more reliable in terms of evidentiary material. However, this assumes the integrity of the electronic data has been preserved in advance of the analysis and not been compromised by others with access to the electronic media prior to the analysis.

In some cases, the most compromising data can be found in deleted files that can be restored by skilled investigators using integrated data recovery software, such as EnCase, FTK, X-Ways Forensics etc.

3. Identify and analyse relevant contracts and other documents reflecting ownership

Another important step in tracking down and recovering stolen assets is the identification, compilation and analysis of documents, such as sales, credit and other contracts, articles of association, deed of partnership and statutes, financial statements, court orders, legal and bankruptcy filings and other relevant documents indicating that the title to assets or funds exists or, at least, is claimed by the respective party.

This step needs to be taken in order to verify the legal owner of a specific asset and when the title to the asset was established. The aim of this procedure is to establish a 'pedigree' for the specific asset or find out about the underlying documents of a certain transaction.

There are numerous potential locations for these documents. The first location is often the fraudster's office. Fraudsters often feel confident that their asset misappropriation scheme will never be detected and they do not take steps to cover their tracks and destroy relevant documents. Thus, searching the office of a suspect is always a potential success factor in securing relevant documents.

The documents at hand do not only have to be analysed in terms of their content and the identity of the contracting parties but also from a forensic standpoint to identify signs of document falsification or forgery. Indicators for falsified documents include, for instance, signs that signatures have been scanned or photocopied, pages removed or subsequently amended, contract dates appear to be out of sequence from a chronological perspective etc. Sometimes even a missing date of signature is an

indication that the document may have been created at a later stage in order to cover up the misappropriation of assets.

What is of further interest upon analysing contracts is the definition of the contractual object. The less definite the contract details are with regard to the services to be rendered, the higher the probability that these contractual gaps are used in order to misappropriate funds. The same applies to the terms of the contract, i.e., when the lifespan of the contract is left open.

Contracts and other documents can also give the investigator an indication of when incoming and outgoing payments are due to appear in the accounting systems, i.e., at what date, and which amount is supposed to be documented in the creditors and debtors balances. The investigator can single out payments accordingly that are either made based on a suspicious contract or that are made in the absence of any underlying contractual relationship at all. The investigator is thus required to look into the bank statements and corresponding accounting documents in order to identify relevant transactions.

4. Analyse bank account statements and accounting documents

Analysis of banking and accounting records is a critical part of every asset tracing investigation, especially when it is funds that are to be tracked. Before looking into the bank account statements, the investigator should ensure that all relevant bank accounts have been identified and are taken into account in this part of the process. Thus, the first task for the investigator is to request a complete list of all bank accounts held with the relevant banks throughout the review period. Upon receipt of the list, the investigator can identify the potentially relevant bank accounts for the investigation, e.g., off-shore bank accounts, bank accounts with large transaction amounts etc.

Based on this list, the investigator requests the bank statements and corresponding transfer balances for the identified bank accounts in order to gain an insight into the transactions made within the review period. This, of course, depends on the authority needed or available to secure these records which, in some instances would be derived from the holder of the account and in others from law enforcement. Depending on the particular jurisdiction, in which the asset is to be traced, legal means such as freezing or disclosure orders may come into play as well. By using the latter, a bank may even be compelled to disclose the account data.

After receiving and reviewing the bank statements in respect of potentially suspicious transactions, the actual tracing of funds involving the different bank accounts commences. The difficult task for the investigator at this point is to identify the commingled funds and categorise them as either apparently appropriate transactions or suspicious looking transactions. The basis for the identification of suspicious transactions may include information derived from the intelligence gathering process, the contract analysis, electronic file reviews, interviews conducted with third parties and other information.

At this stage, the investigator may only have indicators in respect of improper transactions that must now be proven by tracking the suspicious looking transactions to the beneficiary. This is primarily done through charting tools, such as in the intelligence gathering process, in order to be able to follow the trails of the funds through the jungle of numerous bank accounts. By establishing connections between the different flows of funds, previously unknown bank accounts can be identified that may provide new leads on the remainder of the funds.

In the case of large volumes of transaction data, the use of forensic technology software is to be considered in order to minimise the workload for the investigator. In

this case, the software, such as Account Analyser, ACL, InfoZoom, IDEA and others, is used to identify patterns and anomalies in the transaction data provided. These tools can also be used to examine the corresponding accounting data by highlighting debit and credit entries in the accounting system. What is particularly interesting in this instance is the question as to how the suspicious looking bank transactions have been accounted for in the accounting process as these are, for example, covered up by false debit entries to an expense account.

5. The human factor: conducting interviews – witnesses and other informants

As in the intelligence gathering process, conducting interviews should be an ongoing part of the asset tracing investigation as more and more information becomes available. This can, in turn, be used for further interviews or in deciding who to approach for further information.

As distinguished from, for example, open source intelligence which is considered a secondary research methodology, interviews constitute primary research by their very nature. Not only does one gain direct access to a person, interviews also open up ways to read between the lines, i.e., to understand the unwritten parts of, for example, a contract, answering the 'why'-question.

Generally, interviews are conducted in order to fill in the informational gaps that remain after completion of the link, electronic file and document/transaction analysis (refer to previous section). These gaps may remain because not all the details relevant for identifying the location of the stolen assets are available through the analysis of documents. The fewer the documents and available data, the more the investigator is dependent upon interviews with informants who point one in the right direction to continue searching.

An interview is therefore considered to be a quasi formal conversation that consists of, at least, three main parts/phases, i.e., the preparation, interview and documentation. In order to avoid accusations of misconduct on the part of the investigator, such as the use of undue influence or pressure, during one of these phases, it is considered best practice always to hold interviews with at least two interviewers. This also, for example, assists in safeguarding findings that may be derived from such interviews at subsequent proceedings, e.g., being labelled as hearsay before a court. An ongoing discussion that is also largely dependent on the jurisdiction in which an investigation takes place concerns the transcription and documentation of an interview. Depending on the critical nature of the evidence provided by the interviewee, interview summaries bearing the original signature of the interviewee, in some jurisdictions, are also considered best practice.

Without going too deeply into the wider field of interviewing, some important aspects should also be borne in mind when answering the 'who's' and 'how's' during the course of an investigation:

Especially useful are contact persons who actually have a stake in the asset and therefore in the success of the investigation. What has also proven to be effective is the conducting of a confrontational interview with the fraudster. As fraudsters are generally reluctant to pass on information that might lead to their own conviction, this approach can only be adopted if the fraudster is obliged to cooperate under the terms of a valid employment contract with the client.

If the interview is prepared and conducted by experienced interviewers, the fraudster may give leads to the location of assets or funds without even realising it. Also seemingly insignificant remarks given by the fraudster can be helpful in providing the missing pieces of information that the investigator was unable to obtain by analysing

documents and other sources. The more critical an interview is to the investigation, the more time should be spent on its preparation. Useful tools in this instance are interview guides that provide an outline of the subjects, questions and documents used during the interview. In particular, the timing when to present critical and compromising documents during an interview should be well prepared and planned.

IV. Limitations in conducting private asset tracing investigations

Various restrictions and limitations apply to asset tracing investigations. They stem from legal requirements, such as the provisions of data protection legislation, which have to be taken into account in the course of an investigation. What complicates the matter significantly is that different countries have different jurisdictions, therefore requiring the observance of varying legal requirements. Furthermore, there are also financial aspects, such as a simple cost-benefit-ratio, that have to be borne in mind when embarking on an asset tracing process.

1. General legal restrictions and limitations

Legal restrictions in various countries can either have an effect on the way an asset tracing investigation is conducted or on how the findings can be used in court. The latter is mostly dependent upon how the evidence has been produced, and this is again a matter of how the investigation was carried out.

Generally speaking, every successful asset tracing investigation must comply with the legal requirements that are set out in different laws, such as, for example, the various data protection acts in different jurisdictions.

But within every limitation, there is always a purpose to be served if the investigating company assures compliance with these legal restrictions, e.g., The investigating company does not expose itself to any legal liability that can arise from inappropriate handling of an investigation and the results of the investigation can be used in legal proceedings.

As the many diverse jurisdictions and their legal requirements are too numerous to be covered in this short chapter, the following section uses, for illustration purposes, the legal restrictions imposed on the private investigator by German privacy laws. Before conducting an asset tracing investigation, the investigator should consult the local laws of the relevant jurisdiction(s).

2. Legal limitations example: Germany

In terms of the process of an asset tracing investigation as described above, this has the following implications for the investigator:

The analysis of e-mails, electronic documents and files obtained from searching the suspect's office, for example, entails potential restrictions imposed by privacy and data protection legislation. These become effective if the fraudster is, for example, an employee of the client requesting an asset tracing investigation. Generally, it is not permissible to examine personal documents and belongings without the explicit consent of the respective employee who owns such items. However, if there are strong indications that an individual whose personal items are to be examined has committed a criminal offence, the investigation of personal belongings also may actually be

continued. This can be relevant in cases when important contracts or documents containing transactional data are stored in the office of the suspect employee and required in order to conduct the contract and transaction analysis. It is often difficult to differentiate between personal and business related documents as this can only be discovered upon inspecting their content.

The same applies to electronic data stored on the computer hard drive of the suspect employee as well as to files contained on the company server. In this case, electronic data (e.g., e-mails, files etc.) is only allowed to be examined if its content is business related. Personal documents are generally not permitted to be analysed, unless the employee has signed a respective clause authorising the examination. Such a clause can form part of the employment contract, for example, or of the company wide policy prohibiting the private use of company computers to which the employee has agreed upon signing the employment contract. Only in these cases is the analysis of personal documents permitted within the legal boundaries of the German Data Protection Act (Bundesdatenschutzgesetz).

Due to these legal restrictions, however, important information contained in personal documents may not be considered in developing a case during an asset tracing investigation unless the fraudster agrees to the examination. In modern society, personal and professional lives are often entangled, significantly increasing the challenges for the investigator to secure the evidence necessary to successfully manage the asset recovery process.

Other potential limitations, such as employment issues, may arise when client employees are interviewed. If the fraudster is an employee of the client, it is generally necessary to confront him with evidence and facts collected during the investigation. As already described above, generally speaking, the employee is obliged to answer the questions asked by his employer or by the investigator authorised to do the interviewing for the employer. Even though the obligation to cooperate with the investigation generally derives from an existing employment contract, the employee may still refuse to answer if this would result in self-incrimination.

3. Organisational limitations

The intelligence gathering process can only be as effective as the sources available for obtaining the relevant information on individuals and entities. However, access to the correct data can be challenging as, for example, open source databases are not always regularly updated. Therefore, limits can be set, based on whether the information that is available is actually up to date and ready to use. This becomes a critical success factor, for example, if the information provided is used in order to determine the title to assets that are under investigation.

Another important restriction in using open databases is that certain information is simply not available. This becomes an issue, for example, if there are trustees holding interests in a shell company. In this case, the flow of funds can only be traced to the respective entity and to the participating trustees. However, the 'real' investors in this entity are generally not disclosed. The same applies to silent partners who do not have to publicly disclose their interests.

In both of these open source database instances, researching publicly available databases simply does not lead to the desired results. The investigator must think of other ways of obtaining the required information, such as examining e-mails, electronic files and documents that may result in leads to the individuals under investigation.

Another important aspect in this instance would be that the available transaction data is simply not yet properly edited to enable the processing of the data for further analysis using e-discovery or data mining tools. The same applies to physical documents, such as bank statements that may not be available from the banks because of banking secrecy laws in the event that the client is not the owner of the bank accounts that need to be analysed.

4. Economic limitations

Economic limitations are defined by the damage to the organisation measured in terms of the value of the stolen assets compared to the amount of funds required to identify and recover these assets. Due to the fact that recovering stolen assets is an uncertain event that is dependent upon the interplay of several factors, the amount spent on the investigation should logically be less than the value of the stolen assets. Thus, fee arrangements for asset tracing are often based on the percentage of the asset values recovered by the investigator with only the direct expenses incurred for conducting the investigation being reimbursed by the client. Thus, the uncertainty of actually recovering any or all of the stolen assets is shifted to the investigator who, in return, has the potential for achieving higher revenue in the case where the stolen assets are identified and recovered.

5. Case study

In order to also provide a more practical insight into asset tracing, the following case about a corrupt government official may illustrate some of the above mentioned challenges:

During one of the regular audits, the local General Accounting Office had noticed that huge amounts of funds had been transferred to off-shore companies using a wide network of subsidiaries. These funds equalling around EUR 50 million, were held in bank accounts pertaining to the aforementioned companies and subsidiaries. Based on this setting, the investigator, an international accounting firm, was engaged by the government in order to recover the stolen assets and funds.

The investigator started the asset tracing investigation by collecting and analysing information on the various entities and individuals involved in the case. The data collected consisted of, for example, trade register data, including relevant background information on directors, company secretaries, founding members, shareholders, bank accounts etc. Another focus was the potential criminal background, including possibly corruption-related offences of the individuals involved in the case. The data collected was transferred to a link-analytical chart in order to visualise the ties between the individuals and entities involved. Wherever information from open sources was not sufficient, on-site inspections were conducted in order to prove the existence of the respective entities in question.

In a next step, the accounting data provided by the client was analysed using tools for mass data analytics. Moreover, paper-printed bank account statements were analysed in order to determine the flow of funds throughout the network of off-shore companies as well as to establish the ownership of the bank accounts. Further actions taken included conducting interviews with witnesses, such as the ex-wife of the government official as well as other informants. However, the human factor, including the availability and accessibility of potential interviewees, was limited because of external pressure from third parties, i.e., the authorities: some of the potential interviewees had already been arrested by the police.

In conducting the asset tracing investigation, the investigator also faced several other limitations. For example, the quality and availability of the accounting and bank account data provided was poor, making it difficult to establish a clear picture of the flows of funds through the network of subsidiaries. The confiscation of accounting records and other documents by law enforcement contributed to the lack of available information that was provided to the investigator for examination. Thus, it was not possible to prove that the stolen funds actually still existed in the bank accounts that were identified as their final destination.

Another limitation facing the investigator was the availability of information on entities based in off-shore countries, and also including countries within Europe (e.g., Liechtenstein).

To overcome all these challenges, creativity was probably the key: win-win arrangements with law enforcement 'helping' the investigator to cope with the large amounts of seized material were only one of many solutions to such challenges.

However, due to the good cooperation with law enforcement and by thoroughly interviewing involved stakeholders, specific legal claims could be prepared, resulting in the potential recovery of assets worth millions of Euros.

V. Conclusion

As described above, the task of tracking down stolen assets is a difficult one, and no asset tracing investigation is like another. There is thus no standard guidance, no roadmap on how to most effectively conduct an asset tracing investigation but one must be fashioned for each unique investigation, informed by the investigator's experience and use of tools to identify, gather and assess information. The process as presented at the beginning of the chapter is merely a rough outline on how to deal with this complex issue. However, this is always dependent upon the setting and circumstances under which an investigation takes place. As assets and funds are transferred around the globe in a manner aimed at concealing their traces, the challenge for the investigator lies in the fact that the settings always change. Thus, it is beneficial for both the investigator and the client to be able to rely on a global organisation of affiliates that are able to join in on the investigation whenever the trail of the stolen assets leads to foreign countries, and therefore to different jurisdictions. But even then, there are numerous challenges and limitations the investigator has to face in order to successfully seize and recover the stolen assets for its lawful owner. However, it is these challenges that make asset tracing a truly interesting and rewarding field for investigators.

ARNO THUERIG*

Case study on asset tracing

I. Case study background

The client adviser of a Swiss private bank transferred approximately USD 1 million through numerous small transactions from his customers' accounts to a third person's bank account at a major United States (US) bank in New York. He achieved this by falsifying the appropriate bank transfer orders and signing them with the forged signatures of each client. In order to conceal his actions, the client advisor did not charge the transactions against the cash holdings of the customers concerned but instead arranged loans in his customers' names at the bank, thereafter using the loan facilities to make the transfers. He secured the customer loan facilities by way of loan guarantees from further unwitting customers. His machinations came to light when the third-party guarantors, who were until then unaware of their guarantee status, were forced by the banks to fulfil their responsibilities. These customers, as well as those whose accounts were debited with the bank transfers, were neither aware of these actions nor had they ever given any such instructions to their client advisor.

As it turned out, after the funds were transferred to the US, they were subsequently forwarded to South America, where they were eventually drawn down in cash at a foreign currency exchange booth. The recipient's name was only known due to the fact that a passport photocopy and mobile phone number were retained by the foreign currency exchange booth.

The client advisor quickly became the centre of the investigation because the transactions were only made possible with his approval. Moreover, an internal bank investigation established that the falsification of the bank transfer orders as well as the guarantee documentation which had been used as security could be fully attributed to him. All this led to the suspicion that the advisor had played a key role and must have had a close relationship with both the US account holder and the final recipient of the funds in South America.

Due to internal resource constraints and the international dimension of the case, the Swiss private bank decided to call in an external forensic specialist to assist in gathering all the facts, and to secure and evaluate relevant electronic data. Decisive factual findings concerning the *modus operandi* and the money transfers, as well as more data about the suspect's actions, were expected, i.e., from an analysis of the transaction flows and examination of the accounts of all the bank customers who fell under the responsibility of this particular bank client advisor.

* Arno Thuerig is a director of KPMG Forensics in Zurich, Switzerland. He is an attorney-at-law and holds a master's degree in Economic Crime Investigation.

II. Forensic technology

Nowadays, no form of economic crime is conceivable without the substantial use of Information Technology (IT). In our global economy, a country's borders are of little significance as information exchange and international payments flow instantaneously from one country to another. The perpetrators operate with greater ease, and preferably internationally, secure in the knowledge that international circumstances present authorities with major procedural problems, thus making international investigations very challenging. Even though the judicial process is currently based on purely physical evidence such as files and documents, which in many places such as Switzerland is still the rule, it is foreseeable that in the not too distant future electronic evidence will become increasingly important for investigative and judicial authorities. Modern methods of communication such as mobile telecommunications, the Internet, e-mails or the Internet-based information platforms such as Facebook, Twitter or Clouds are inevitable in today's business world but, significantly, leave digital tracks. In recent times, an investigator's research has moved from the securing of physical documents to safeguarding electronic evidence data on notebooks, desktops, servers, backup media and mobile communication devices. As a general rule, time is no longer an issue because digital traces tend not to turn yellow and data on network resources – i.e., servers and the Internet – never forget anything. That is why databases, which have long been forgotten or were considered to be (permanently) removed, can become the centre of attention**.** All such data can also be a key source of information and thus significantly contribute towards the success of an asset tracing/asset recovery operation. The seizure and analysis of electronic data from people involved must therefore – in addition to seizing traditional non-electronic data – always be a top priority. The visualisation of digital traces for use in court cases is, of course, also an important factor**.** This process can only be performed by an experienced Forensic Technology team.

III. Corporate intelligence

The most immediate problem in the context of asset recovery remains the gathering of information. With cross-border transactions, the trail can be lost all too easily due to the involvement of various international jurisdictions and other limitations. The affected parties are faced with big challenges, notably in the classic offshore havens and in countries which have little legal stability. Thus, elementary questions about events, payment flows, perpetrators, intermediaries, beneficiaries etc., generally remain unanswered. In this context, globally active companies which provide globally specialised forensic services can provide valuable support through their worldwide network. The instrument for this global information gathering is the so-called Corporate Intelligence Research (CI).

Corporate Intelligence is based on four sources or methods of information-gathering, namely, the 'public domain', the 'closed' and the 'human' sources as well as access to a wide global corporate network. The 'public domain' sources include the official registers such as the commercial register, tax register, land registry and local residents' register, which, in principle, are open to everyone. On the other hand, there are the 'closed' sources. These contain proprietary information, which are regularly accessible only to public authorities or have to be requested by an authorised person. Typically, criminal records are the focus of interest in this instance. In Switzerland, any person can obtain relevant information concerning him-/herself (e.g., as part of the hiring process of a new employer); access to third party information, however, is exclusively

reserved for the authorities. The 'human' sources are represented by private investigators and detectives where their industry specific know-how can be used; they are often hired for specific one-off fact-finding issues. The inclusion of a global corporate network ultimately represents the most powerful instrument for information gathering, particularly in cross-border situations and jurisdictions that demand local knowledge plus an understanding of local customs and legal frameworks. Depending on the country and the legal situation concerned, all these different methods of information gathering can be used, their weighting applied according to the relevant circumstances and providing different levels of results as required.

Initial information on persons, assets and companies can, on occasion, be very limited and insufficient as a basis for further investigation at the outset. For example, a simple 'google' search, which can be conducted by anyone, can quickly lead to some initial information. The completeness, accuracy and context, however, of such free information cannot necessarily be relied upon. Only a combination of the above-described 'public' and 'human' sources can – when combined with the research within a globally active international corporate network and the use of Forensic Technology – complete the picture and represent the key bases for the initiation of international legal assistance proceedings. This is still the most common way to confiscate assets once they have been identified and located.

IV. Action taken in this case

From the very start of the current investigation, all the aspects of Forensic Technology were used simultaneously with the CI searches. Top priority was given to the securing of electronic indications and evidence. The procedure was set up as follows:

1. Identification of evidence

The Forensic Technology team worked closely with the IT managers of the bank, as it was necessary to locate the relevant electronic data storage medium and the relevant data on the bank's own servers. In doing so, the client advisor's corporate notebook, his corporate USB flash drive, his company mobile phone, his e-mail box on the bank's server and his home folder on the departmental server were identified as the relevant media. Simultaneously, as the transaction flows from the Swiss Bank to the US Bank in New York were classified as significant, these too were analysed with the aim to determine whether this was an isolated incident within the bank or whether similar flows from another operation were taking place or had perhaps already previously been processed.

2. Securing the data

The client advisor's notebook and his USB memory stick were imaged by Forensic Technology specialists. This meant creating an identical copy of the hard disk of the notebook and the USB stick. This process also allows partially deleted data to be recovered. In addition, the IT manager of the bank created a copy of the client advisor's e-mail box and his home directory and gave this information to the Forensic Technology team in electronic form. Finally, forensic specialists downloaded the transaction data directly from the bank's systems, in order to locate more information and to track the possible cash flows to the US and identify how they were managed.

3. Analysis of the backed up data

Indexing and keyword search

The initial amount of data which had to be evaluated, was very large. The indexing of the secured electronic data, however, enabled a thorough and efficient search of the databases based on pre-defined keywords. The focus here was on search terms which had some sort of connection with the customer adviser, his environment, the US bank in New York and the South America contact in general. In fact, this method massively narrowed down the relevant data and filtered out significant documents. The interpretation of these documents identified by the search through the employment of specific terms also revealed additional contact details of suspect persons who all resided in the same general location in the South American country.

Graphical representation of the e-mail traffic

The e-mail box of the client adviser was analysed with special software so that the frequency of the correspondence with his associates was visually displayed. It turned out that he had regular contact with the account holder of the US bank. Refined keyword searches with the coordinates of the account holder provided further important information from the documents thus identified. It was also possible to further identify that the client advisor informed an unknown third party about the value date and the exact amount of each transaction, and advised him to collect the cash at the specific foreign exchange booth in a specific South American country. Furthermore, the account holder of the US bank was identified as the sender of these amounts. Moreover, it turned out that in the context of these transactions, the client advisor also had a close connection with the client advisor of another Swiss private bank. Immediate contact with this other Swiss private bank brought an identical pattern of fraud to light. Because of this timely intervention, additional fraudulent acts were prevented at this other bank and further damage was curtailed.

Analysis of the chronology of telephone traffic

The private bank requested their telephone provider to provide the phone call records of the relationship manager's company mobile phone and his company landline connection. These reports also proved that the client advisor had close contact with the holder of the account at the US bank. The same information also resulted from an analysis of the contact information, SMS and telephone bill of his mobile phone, which, in addition, also confirmed his links with the customer advisor of the other Swiss private bank. The communication log, documenting the traffic between the persons involved, was established and the chain of evidence with regard to the suspects completed.

Analysis of transaction data of the bank

The analysis of the bank transaction flows showed that the contact between the client advisor and the US bank and the transaction density were much more intense than previously assumed. This brought other, initially unknown client relationships to light, revealing an identical *modus operandi*.

4. Interaction with the CI team

The interaction with the CI team was characterised by a continuous exchange of information. Background investigations (CI) on the client advisor and his environment, as well as on possible connections between him and the account at a US bank in New York and to the recipient of the funds in South America, provided valuable information. Corporate internal contacts in North and South America in conjunction with CI and Forensic Technology completed the picture obtained in respect of the suspects and their approach. The professional service firm's global network identified decisive evidential leads, which would not have been possible without the knowledge of local practices and familiarity with relevant legislation, and therewith the ability to exercise due respect for the local legal framework and transparency.

V. Asset recovery due to the findings

The successful teamwork of Forensic Technology and Corporate Intelligence allowed for the successful elaboration of the fraudulent acts, the detailed analysis of transaction flows and identification of those responsible. Moreover, within the scope of this fraud case, it was possible to prevent a further bank from suffering collateral damage. Unfortunately, the cash withdrawals from the South American foreign currency exchange booths could not immediately be recovered. Instead, it was possible to successfully determine the person who had collected the cash, thanks to physical on-site inspections. Based on these findings, appropriate legal steps were successfully launched against the client adviser and his associates.

YARA ESQUIVEL*

The United Nations Convention against Corruption and asset recovery: the trail to repatriation

The United Nations Convention against Corruption (UNCAC) came into force on 14 December 2005 and has been signed by 140 countries, of which 137 are parties to the convention.[1] This is not the first effort of the international community to create an international instrument that would oblige the community of nations to adopt measures to prevent and repress corruption. The Organisation of American States, as an example, already in 1996 issued its own Inter American Convention against Corruption, with an emphasis on the importance of regional cooperation.[2] However, UNCAC is innovative in two respects. Firstly, it is the first international instrument that aims to function as a multilateral mutual legal assistance treaty. Secondly, it is the first convention to ever refer to the recovery of assets as a priority in the fight against corruption.

I. Following the trail

According to the World Bank, the cross-border flow of proceeds from criminal activity, corruption and tax evasion is estimated at between USD 1 and 1.6 trillion per year. Tragically, half of this amount is looted from developing and transition economies. USD 20-40 billion dollars of this flow originated in bribes received by public officials from developing and transition countries.[3]

So important is asset recovery under UNCAC that chapter V begins by stating that it is a fundamental principle of the convention.[4] Asset recovery under this treaty is not only considered domestically but also includes the return of assets to a foreign country that has been looted by its corrupt public officials.

The convention calls for the prevention and detection of transfers of the proceeds of crime.[5] This is of special relevance for prosecutors and investigators, as it provides the tools necessary for efficient financial investigations. Art. 52 should be read in

* Yara Esquivel, a former anti-corruption specialist with the International Centre for Asset Recovery (ICAR) in Switzerland is currently posted at the World Bank as an investigator for the Integrity Vice Presidency, with the mandate to investigate fraud and corruption in bank projects.

1 'Signatories to the United Nations Convention against Corruption.' United Nations Office on Drugs and Crime. Web. 06 September 2009, available at http://www.unodc.org/unodc/en/treaties/CAC/signatories.html.

2 'Inter-American Convention against Corruption.' OAS – Organization of American States: Democracy for peace, security, and development. Web. 06 September 2009, available at http://www.oas.org/juridico/english/Treaties/b-58.html.

3 'News & Broadcast - World Bank Unveils Stolen Asset Recovery Initiative.' The World Bank. Web. 06 September 2009, available at http://web.worldbank.org/WBSITE/EXTERNAL/NEWS/0,contentMDK:21299829~pagePK:64257043~piPK:437376~theSiteP.

4 Art. 51 UNCAC.

5 Art. 52 UNCAC.

accordance with the Financial Actions Task Force's (FATF's) 40 Recommendations and 9 Special Recommendations.[6] When applied, these rules allow States to audit transactions even when the assets are transferred overseas. Prevention and control are essential when dealing with asset recovery.

Some preventive measures for money laundering can turn into tools for investigators and prosecutors when dealing with asset recovery. An effective financial investigation is always the first step towards a successful repatriation of assets. It is necessary to establish who received what and how much, as well as where it went to, in order to determine a link between the assets and the criminal offence. Even in civil asset forfeiture, where the standard of proof is on a mere balance of probabilities, causality has to be determined.

Implementing UNCAC's Art. 52 implies several actions, the first being the enhancement of scrutiny of high-risk clients and financial products. An effective 'Know-your-Customer' policy must be applied. This means that financial institutions must verify the data provided by their clients and determine the beneficial owner of their accounts, with special regards to politically exposed persons (PEPs).

The FATF's 40 Recommendations and 9 Special Recommendations recommend the following customer due diligence measures:

- Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information
- Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements, this should include financial institutions taking reasonable measures to understand the ownership and control structure of the customer
- Obtaining information on the purpose and intended nature of the business relationship
- Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds

There is no argument about the heightened scrutiny to which a PEP is subject – the problem that most countries face is the broadness of the definition. According to the Wolfsberg Group, this is a person who performs important public functions for a state[7] but the definition is still very broad and allows for interpretation. Several examples are provided. The Swiss Financial Market Supervisory Authority defines it as a person occupying an important public function[8], the United States (US) inter-agency guidance defines it as a senior foreign political figure[9] and the Bank for International Settlements has simply defined these people as 'potentates'[10]. The precaution should also be extended to people who are close to PEPs, such as their families and

6 'Financial Action Task Force (FATF).' Organisation for Economic Co-operation and Development. Web. 06 September 2009, available at http://www.fatf-gafi.org/pages/0,3417,en_32250379_32236920_1_1_1_1_1,00.html.
7 'Wolfsberg FAQ's on Politically Exposed Persons.' Wolfsberg AML Principles. Web. 07 September 2009, available at http://www.wolfsberg-principles.com/faq-persons.html.
8 Ibid.
9 Ibid.
10 Ibid.

associates. But then, how do we define 'family' or 'close associate'? The third EU AML Directive contains a definition of 'family'.[11]

To mitigate some of these problems, paragraphs 5 and 6 of Art. 52 of UNCAC recommend the establishment of disclosure systems for public officials. This means that governmental agencies must be given the authority to administer and manage such a system with consideration given to the sensitivity of the information.

Special attention should be paid to financial products that raise attention by their own nature, such as when the client does not coincide with the beneficial owner (joint accounts, joint securities accounts, investment companies and other collective investments), offshore companies, clients holding assets without specific beneficial owners (e.g., discretionary trusts), or clients bound by professional confidentiality (attorneys or notaries holding accounts for specific professional purposes).

Record keeping is key to investigations. A strong banking system is essential. If financial institutions keep accurate records of their transactions for a sufficient amount of time, assets can always be traced. It is important to remember that money always leaves a trail, unless it is transferred in cash. This goes hand in hand with the requirement to share information with competent authorities in other State Parties. Some financial intelligence units are familiar with this data sharing system[12] and their experience could be helpful when extending the model to law enforcement agencies.

A challenge is posed in those countries for which a professional banking system is in its infancy, and there is no sophisticated banking culture in place. In such countries, large currency transactions still take place and might complicate the task of following the money. However, when the beneficiaries of the corrupt activity attempt to enjoy these illegal gains overseas, they always have to use the traditional banking system.

II. When the trail leaves home

When Professor Theodore Levitt coined the term 'globalisation' in 1983, referring to world markets[13], little did he imagine that this phenomenon would affect every aspect of social organisation. Globalisation has clearly affected the way criminals conduct their business and the way law enforcers and jurists must conduct their investigations. Organised crime has transcended traditional boarders with the aid of technology, posing an important challenge for prosecutors and investigators.

Several aspects of technology have facilitated the globalisation of crime. The communications network has turned the world into a very small place, where telephone calls, e-mails, text messages and faxes have eliminated the distance between people. This improvement in the communication system has led, at the same time, to a growth in international commerce and banking. Through wire transfers via Internet banking, letters of credit, automated teller machines, e cash, credit and debit cards and countless other tools, we are able to move enormous amounts of money in seconds from one place to the other, done in some cases with great discretion and anonymity. These developments have made it easy for criminals to conduct their activities and harvest their earnings in one region of the world and hide them in a different one.

11 http://ec.europa.eu/internal_market/company/financial-crime/index_en.htm.
12 See Principles of Information Exchange, available at: www.egmontgroup.org.
13 Levitt, Theodore. 'The globalization of markets.' McKinsey Quarterly 1984. McKinsey Quarterly. Web. 7 September 2009, available at http://www.vuw.ac.nz/~caplabtb/m302w07/Levitt.pdf.

The last decades have seen law enforcement struggle to solve the challenges posed by the elimination of borders. Traditionally, letters rogatory were the customary method to obtain legal assistance from overseas in criminal matters. These are formal communications from the judiciary of one country to the judiciary of another country requesting the performance of an act typical of a criminal investigation.[14] However, letters rogatory take a large amount of time. They are extremely formal, which means that they must contain all official signs from the requesting country such as stamps, signatures, etc. To guarantee their authenticity, they must be signed by a person whose signature has been registered and they must be transmitted through the diplomatic pouch from the Ministry of Foreign Affairs of the requesting country to its embassy or consulate in the requested country, and then on to the national authorities. This process can take an extreme amount of time, and must be repeated on the way back in order to respect and maintain the chain of custody. Clearly, in modern day investigations, when money can be wire transferred at the click of a mouse, this system is becoming obsolete.

Mutual Legal Assistance (MLA) treaties have addressed this problem. They are more expeditious and require less formality, always keeping in mind the respect for the other country's sovereignty and the chain of custody. Each country designates a central authority for direct communication. By eliminating the middleman (the Ministry of Foreign Affairs), requests can be transmitted more swiftly and the communication become clearer.

But what happens when two countries do not have in place an MLA treaty? It is worth going back and reviewing the provisions that the convention has established regarding this topic in Art. 46. UNCAC functions as a multilateral treaty for mutual legal assistance. This is key, as State Parties to UNCAC are not required to send letter rogatories through the diplomatic channels to foreign authorities. It is sufficient to send a mutual legal assistance request to the central authority under the formal requirements listed within this instrument.

The convention has established that mutual legal assistance can be used, apart from the traditional purposes, for the recovery of assets. The mutual legal assistance request is subject to some formality, according to Art. 46. It must clearly establish the identity of the authority making the request and the subject matter and nature of the investigation. It should also contain a summary of the relevant facts and a description of the assistance sought. It must also mention the identity of the people involved. Finally, it should establish the purpose for which the information will be used. The letter of request must be sent in a language acceptable to the authorities of the requested party. The lack of any of these requirements is reason enough to refuse assistance.

When dealing with mutual legal assistance, there are several aspects that must be emphasised. The first is the goal of the request. If the goal is to gather evidence that will later be incorporated into a criminal process and admitted in court, this evidence must be protected at all costs. That means that it should be gathered in accordance with the general principles of criminal law, and the chain of evidence must be respected. Countries can, and should, include in their requests any special procedures needed for the gathering of evidence. This is especially challenging when it comes to interviewing witnesses. The principle of cross-examination should not be forgotten. UNCAC is innovative in the sense that it suggests the use of technology to overcome this problem, and the use of video conferencing is presented as an option (see Art. 32 of UNCAC). The second aspect to be considered is dual criminality. Requesting countries must ensure to qualify the conduct investigated under conduct that is

14 'Preparation of Letters Rogatory.' Welcome to Travel.State.Gov. Web. 07 September 2009, available at http://travel.state.gov/law/info/judicial/judicial_683.html.

considered a criminal offence in the requested country. Requested countries should also remember that if the fact pattern fits conduct considered by it as a criminal offence, the nomenclature should not matter. Precious time is wasted when this is overlooked. Finally, the principle of specialty must be respected. This means that the evidence gathered can only be used for the purposes described.

III. A victimless crime?

Traditionally, corruption offences have been perceived as victimless crimes. The average person does not feel affected by the funnelling of public monies into the pockets of dishonest public officials, when in reality corruption hampers development. In fact, corruption offences affect the life of the individual far more than what is perceived, as it deviates public funding from social projects, public infrastructure or general governmental administration. These are crimes that affect everyone. The UNCAC recognises State Parties themselves as victims of corruption and as such, they hold the right to recover property that has been sent overseas.

Art. 53 was designed to ensure that State Parties have in place a wide range of legal remedies to recognise other State Parties as having legal standing to initiate civil actions and other direct means to recover illegally obtained and exported property. These may include:

- As a plaintiff in a civil action. State Parties should review the requisites for accessing the Courts when the plaintiff is a foreign country, since in many jurisdictions this may trigger jurisdictional and procedural issues
- As a party recovering damages caused by criminal offences. Proceeds from corruption should be recovered only on confiscation grounds, and State Parties are obliged to enable their Courts to recognise the rights of victim States Parties to receive compensation or damages. This is relevant to offences that have caused loss in a different State Party to which the offence has been tried
- As a third party claiming ownership rights in a confiscation procedure, being it either civil or criminal. As a victim state may not be aware of the procedures undertaken, State Parties should consider notifying the victim country of its right to stand and prove its claim

Once identified, assets must be repatriated. In order to achieve this, effective international cooperation is a basic requirement, an aspect to which UNCAC refers in Art. 54. A challenge to this topic is the recognition of foreign confiscation orders. Traditionally, the element of extra-territoriality was denied in respect of confiscation orders, as this implied the nationalisation of private property. However, the trend seems to be changing.

Art. 54 requires State Parties to adopt procedures that allow the enforcement of a confiscation order. This could be achieved through the recognition of the foreign order and direct enforcement, as well as the institution of new proceedings according to the domestic law to that effect.

Historically, the proceeds of corruption cases have been recovered under money laundering charges in the jurisdiction where the proceeds of crime were hidden. Para. 1(b) of this Art. requires State Parties to ensure their ability to confiscate the proceeds of foreign predicate offences when investigating money laundering. This paragraph also opens the possibility for State Parties to establish proceedings for confiscating illegally gotten assets, such as an *in rem* action.

UNCAC recommends the adoption of a remedial procedure for cases in which a criminal conviction cannot be obtained, i.e., when the defendant has died, fled, etc. For these cases, the drafting of a civil asset forfeiture law seems to be the most appropriate solution.

IV. The sum of all elements

As mentioned above, international cooperation is fundamental in international asset recovery. Hence, Art. 55 requires the establishment of an international cooperation regime specifically for the purpose of confiscation. UNCAC reiterates the importance of the enforcement of foreign confiscation orders as well as the adoption of preventative measures while the orders are being enforced.

For the purposes of confiscation, UNCAC requires its signatories to adopt measures to allow their competent authorities to adopt provisional measures at the request of another party in order to protect a potential confiscation, such as the possibility of obtaining a domestic freezing or seizing order upon request.

Once this has all been taken care of Art. 57 of UNCAC clearly establishes the rules under which all recovered assets must be returned to the requesting country, under three different scenarios.

Para. 2(a) deals with property that proceeds from the embezzlement of public funds or the laundering of these assets, described by the convention in Articles 17 and 23. As there is no doubt that the requesting State is the victim of the offence, the convention establishes that the assets must be returned to it. The State, like any other victim, has the right to demand that the proceeds are returned.

In the case of any other proceeds covered by UNCAC (Para. 2.b), the requested party will return the assets under the following situations:

- When the requesting State has reasonably established its prior ownership of the confiscated property (e.g., bribes paid with public funds)
- When the requested State recognises damage to the requesting State as a basis for returning the confiscated property (e.g., when the State has acquired overpriced property in order to conceal an illicit advantage obtained by one of its officials)

Finally, para. 3(c) provides that in all other cases, priority should be given to the return of confiscated property to the requesting State when it will go to its prior legitimate owners or to compensate the victims of the crime.

It is important to keep in mind that UNCAC provides the guidelines to be incorporated in the States Parties' legislation in order to simplify the work of prosecutors and investigators when working corruption cases.

Asset recovery cannot be isolated. There are several steps that cannot be skipped. An effective financial investigation will lead to the assets to be recovered, and give the requested country the reasons for which they should be repatriated. A thorough knowledge of how to draft mutual legal assistance requests is also required, as this will speed up the proceedings overseas and the UNCAC is an efficient tool for requesting assistance. It is only after a thorough investigation and effective international cooperation that assets can be confiscated and ultimately returned. Repatriation can only occur at the end of a strong investigation.