



© 2015 Basel Institute on Governance, International Centre for Asset Recovery

Basel Institute on Governance, Steinenvring 60, 4051 Basel, Switzerland  
[www.baselgovernance.org](http://www.baselgovernance.org), [info@baselgovernance.org](mailto:info@baselgovernance.org)

Responsibility for the views expressed and for any errors of fact or judgment rests with the authors alone.

# Tracing Illegal Assets - A Practitioner's Guide

International Centre for Asset Recovery



# Contents

Contributors 9

Basel Institute on Governance 13

Acronyms 15

## 1. INTRODUCTION 19

## 2. CASE STRATEGY AND INVESTIGATION PLANNING 23

1. Introduction 25
  2. Tracing stolen assets – A multifaceted task 25
  3. Setting up an investigation team 26
  4. Formulating and initiating the overall case strategy 27
  5. Creating an investigation plan 27
    - 5.1 Outlining the features of the offences 28
    - 5.2 Creating an evidence matrix: Outlining the evidence to be gathered and the method to gather it 29
    - 5.3 Outlining a media communication strategy 40
    - 5.4 Outlining case evaluation procedures 41
  6. Remember the priority 41
- Chapter checklist: Creating an investigation strategy 41

## 3. FINANCIAL PROFILING 43

1. Introduction 45
  - 1.1 A tool to provide indirect or circumstantial evidence 45
  - 1.2 A tool to prove the crime of ‘unexplained wealth’ or ‘illicit enrichment’ 46
2. Source and Application of Funds analysis to evaluate unexplained income 46

## 4. MUTUAL LEGAL ASSISTANCE 51

1. Introduction 53
2. Step 1: Preparing for mutual legal assistance (MLA) 54
  - 2.1 Before initiating MLA: Intelligence gathering and informal methods of cooperation 55
  - 2.2 When to request MLA: Timing of the request 55
  - 2.3 How to request MLA: Legal basis 56
  - 2.4 What to request through MLA: Types of assistance 57
  - 2.5 How to request MLA: Dual criminality 57
  - 2.6 How to request MLA: Speciality 58

- 3. Step 2: Drafting MLA **58**
  - 3.1 Final consideration: Fishing expedition **59**
  - 3.2 Language of the request **59**
- 4. Step 3: Submitting a request for MLA **59**
- Annex 1 - MLA checklist **61**
- Annex 2 - Model request for MLA **63**

## **5. USING THE ANTI-MONEY LAUNDERING FRAMEWORK IN ASSET TRACING 67**

- 1. Introduction **69**
- 2. The anti-money laundering (AML) framework **70**
- 3. The use of AML suppressive measures in asset tracing **72**
  - 3.1 Provisional measures **72**
  - 3.2 Provisional measures for cases with an international dimension **72**
  - 3.3 Confiscation and the reversal of the burden of proof **73**
  - 3.4 Non-conviction based confiscation **74**
  - 3.5 Range of assets subject to freezing, seizing and confiscation **75**
- 4. The use of AML preventive measures in asset tracing **75**
  - 4.1 Requirements in customer due diligence (CDD) and record keeping **76**
  - 4.2 Identification of politically exposed persons (PEPs) **78**
  - 4.3 Targeted financial sanctions related to individuals and entities **79**
- 5. The role of the Financial Intelligence Units (FIUs) in asset tracing **80**
  - 5.1 Types of FIUs **80**
  - 5.2 Reporting obligations and information received by FIUs **82**
  - 5.3 The role of FIU in financial investigations and adding value to data **84**
  - 5.4 Dissemination of information to other authorities **87**
- 6. The role of national and international cooperation in asset tracing **88**
  - 6.1 Cooperation at national level **88**
  - 6.2 Cooperation at international level **89**

## **6. THE USE OF CORPORATE VEHICLES TO CONCEAL ILLEGAL ASSETS 93**

- 1. Introduction **95**
- 2. What is a corporate vehicle? **96**
  - 2.1 Meaning of offshore **97**
  - 2.2 Role of trust and corporate services providers **98**
- 3. Beneficial ownership **99**
- 4. Typical corporate vehicles used for criminal purposes **99**
  - 4.1 Shell companies **100**
  - 4.2 Shelf companies **102**
  - 4.3 Trusts **104**
- 5. Establishing control and benefit **108**

- 5.1 International cooperation 109
- 5.2 Relevant documentation/information 110

## **7. TRACING DIGITAL CURRENCIES 113**

- 1. Understanding digital currencies 115
  - 1.1 General characteristics 115
  - 1.2 Where are one's bitcoins? 116
  - 1.3 Legislative characteristics 117
- 2. Tracing digital currencies 118
  - 2.1 Digital currencies and criminals 118
  - 2.2 The blockchain as an investigative tool 119
  - 2.3 Investigative techniques 119
  - 2.4 Case study: Silk Road 122
- 3. Final considerations 124





# Contributors



PHYLLIS ATKINSON is Head of Training at the International Centre for Asset Recovery, providing technical assistance to developing and transitional countries through the design, development and delivery of interactive, practical and participant-based training workshops on anti-corruption, anti-money laundering, financial investigations and asset recovery. (Editor and contributor)



ELENA HOUNTA is a Senior Asset Recovery Specialist at the International Centre for Asset Recovery, assisting jurisdictions, mainly in Sub-Saharan Africa and South America, in developing strategies relating to money laundering and corruption cases with a view to recovering the proceeds of crime and establishing effective anti-money laundering and anti-corruption mechanisms. (Editor and contributor)



SELVAN LEHMANN is AML/CFT Specialist & Project Manager Basel AML Index at the International Centre for Asset Recovery and responsible for managing the Basel AML Index. He is also assisting in case consultancy work in Eastern Europe/Central Asia and on various technical anti-money laundering and asset recovery projects. (Editor and contributor)



CHARLES MONTEITH is Head of Legal and Case Consultancy at the International Centre for Asset Recovery, leading the team in advising a broad range of countries on asset recovery cases as well as reviewing legislation and the institutional capacity of countries in relation to anti-corruption and asset recovery and facilitating related reform processes. (Editor and contributor)



ANDREW DORNBIERER is an Asset Recovery Specialist at the International Centre for Asset Recovery, working on case investigations in Sub-Saharan Africa and assisting with legal anti-corruption and asset recovery reviews as well as AML/CFT country studies.



PEDRO GOMES PEREIRA is a Senior Asset Recovery Specialist at the International Centre for Asset Recovery, working on cases in South America, South East Asia and the Middle East and providing legal expertise to countries in preventing and combating corruption and money laundering, specialising in MLA, extradition and international legal and investigative strategies.



FEDERICO PAESANO is a Senior Financial Investigation Specialist within the Training division of the International Centre for Asset Recovery, delivering technical training programmes on financial investigations and asset recovery in South America, Africa, Asia and Europe and drafting operational manuals for law enforcers.

For more information on the professional experience of the contributors, please visit: [www.baselgovernance.org/about\\_us/team](http://www.baselgovernance.org/about_us/team).

We would like to thank Amanda Dooley, freelance editor, Nina Schild and Peter Huppertz from the Basel Institute on Governance for their dedicated work and invaluable support in publishing this Guide.





# Basel Institute on Governance

The Basel Institute on Governance is an independent non-profit competence centre specialised in corruption prevention and public governance, corporate governance and compliance, anti-money laundering, criminal law enforcement and the recovery of stolen assets. Based in Switzerland, the Institute's multidisciplinary and international team works around the world with public and private organisations towards its mission of combating financial crime and tangibly improving the quality of governance globally.

The Basel Institute is composed of four divisions: the International Centre for Asset Recovery (ICAR), the Division for Public Governance, the Division for Corporate Governance and Compliance, and the International Centre for Collective Action (ICCA).

The International Centre for Asset Recovery (ICAR), founded in 2006, assists authorities in enhancing their capacities to seize, confiscate and recover the proceeds of corruption and money laundering through strategic case advice, technical assistance and capacity building. ICAR's training programmes are based on a unique, practice-oriented and interactive methodology that in each case is tailor-made to the concerned country's needs, its laws and institutions. ICAR's training programmes include all the issues covered in the chapters of this guide. In addition, ICAR operates a web-based information and knowledge-sharing platform: [www.assetrecovery.org](http://www.assetrecovery.org)



# Acronyms

AML	Anti-money laundering
ARINSA	Asset Recovery Inter-Agency Network of Southern Africa
ARIS	Asset Recovery Intelligence System
BTC	Bitcoins
CARIN	Camden Assets Recovery Interagency Network
CDD	Customer due diligence
CFT	Countering the financing of terrorism
DNFBP	Designated non-financial businesses and professions
EU	European Union
FATF	Financial Action Task Force
FBI	Federal Bureau of Investigation
FI	Financial institution
FinCen	Financial Crimes Enforcement Network
FIU	Financial Intelligence Unit
FSF	Financial Stability Forum
IBC	International business corporation
ICAR	International Centre for Asset Recovery
ICIJ	International Consortium of Investigative Journalists
IRS	Internal Revenue Service (USA)
IP	Internet protocol
IT	Information technology
KYC	Know your customer
LEA	Law enforcement agency
MLA	Mutual legal assistance
MoU	Memorandum of understanding
NRA	National risk assessment
OECD	Organisation for Economic Co-operation and Development
OFPC	Office of Foreign Assets Control
OFC	Offshore financial centre

PEP	Politically exposed person
RBA	Risk based approach
SAR	Suspicious activity report
StAR	Stolen Asset Recovery Initiative
STR	Suspicious transaction report
TCSP	Trust and company service provider
UNCAC	United Nations Convention Against Corruption
UNSC	United Nations Security Council
UNTOC	United Nations Convention Against Transnational Organised Crime







# 1. Introduction

When pursuing the perpetrators of a crime, law enforcement officers will usually have one focus: to identify the perpetrators and incarcerate them as punishment. Financial crime, however, is unique from many other crimes in that the major motivating factor behind such crime is personal enrichment. Consequently, perpetrators of these crimes are quite prepared to serve prison sentences if their newly stolen wealth is still available to them to enjoy upon their release. In order to effectively tackle financial crime and reduce the incentive for criminals to commit this type of crime in the first place, the focus of law enforcement officers should not merely be on punishing the perpetrators but also on identifying and tracking the criminal proceeds that have been generated and acquired.

Therefore, the first fundamental priority for law enforcement authorities dealing with financial crime is to always seek to recover illegally obtained assets. This will effectively strip the perpetrators of the gains of their crime and will act as a significant deterrence for future perpetrators. Furthermore, the eventual return of stolen assets, especially in corruption offences, will have a significant impact on the overall development of a country, as these returned assets could be used to invest in essential social services and development projects.

Asset recovery is a process in which each stage is dependant upon the prior stage being properly conducted. Poor intelligence makes it very difficult, if not impossible, to mount a successful investigation, and a weak investigation makes it very difficult for a prosecutor to win a case in court. In other words, the better the earlier stages are done, the greater the chances of success. The complexity of asset recovery processes and the lack of technical knowledge often observed in developing countries are major hindrances to successful asset recovery.

The recovery of illegally obtained assets, however, requires first the need to successfully trace them. Asset tracing refers to the process whereby an investigator identifies, tracks and locates proceeds of crime. Investigators trace assets for the purpose of seizing and/or freezing them,

so that these assets can be confiscated through a judicial order and ultimately returned to the victims of the crime – be it a private party or the state. In a traditional asset tracing investigation, there are three objectives: locating the assets, linking them to an unlawful activity so as to obtain freezing and confiscation orders, and proving the commission of the relevant offences. These should not be considered as three distinct and separate steps, but as overlapping objectives that investigators should work towards simultaneously for the purpose of achieving a final goal: to deny criminals the proceeds of their crime.

This publication, ‘Tracing Illegal Assets’, written by practitioners, takes a practical rather than a theoretical approach to tracing illegally obtained assets, and it emphasises the intelligence and investigatory aspects of asset recovery. Our direct audience is mainly those with a law enforcement background, including prosecutors. Other practitioners in the field, such as lawyers, financial advisors, investigative journalists and activists, will also find this publication useful. Although the court process is not directly covered, this publication will be of particular interest to prosecutors who are increasingly involved in investigations from the outset and will also need to know how to handle intelligence. All are referred to as practitioners in this guide unless it addresses a specific target group, such as investigators.

In general, the process that leads to the recovery or repatriation of assets is divided into four basic phases:

- Pre-investigative phase, during which the investigator verifies the source of the information initiating the investigation and determines its authenticity. If there are inconsistencies or incorrect statements and assumptions, then the true facts should 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 through, for example: financial investigations to establish the

financial profile of the suspect, the use of preventive measures provided by the anti-money laundering legal framework, mutual legal assistance (MLA) requests to obtain information relating to offshore structures. 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.

As indicated above, we cover the first two stages. Several other publications already provide useful case studies and extensive handbooks addressing the overall asset recovery topics.<sup>1</sup>

Practitioners will benefit from an easy-to-understand guide that leads them through the key and critical steps by stressing the strategic considerations as well as crucial 'check-lists' for a successful asset recovery case. The chapters described in further detail below address mainly the pre-investigative and investigative stages, the mutual legal assistance process, and the freezing or seizure of assets through the use of the anti-money laundering (AML) framework. Additionally, the use of offshore vehicles and digital currencies is covered.

Chapter 2 addresses how investigators dealing with complex

asset recovery cases will generally have to compile and sift through a large amount of information to successfully identify and track proceeds of crime. When investigators are faced with an overwhelming amount of information located in several jurisdictions, it is easy to lose sight of the main purpose of an investigation and to forget this first fundamental priority. It provides, therefore, a structured method for an effective investigation strategy and plan that will assist practitioners in proving essential elements of an offence and increase the capacity to successfully identify and track proceeds of crime.

During the investigative phase and as part of the investigation plan and strategy, a very important tool that can be used to help practitioners establish the link between criminals, their illicit activities and their illicitly obtained assets is the financial profiling of the suspect. Chapter 3 presents a straightforward method of proving unknown income that may be illegal, through the 'Source and Application of Funds' analysis, also known as the 'expenditure', 'funds flow' or 'application of funds' method. The chapter describes how the Source and Application of Funds method can be applied in order to compare, during a defined period of time, the expenditures of a person with his legal and known income. As a result, this method can be used to gather circumstantial evidence for the commission of a crime but also direct evidence in jurisdictions where 'unexplained wealth' or 'illicit enrichment' is criminalised as a stand-alone offence.

Chapter 4 describes in detail the use of MLA, which is an important process in view of the need for international cooperation. Evidence and assets are not always found exclusively in the state conducting the investigation, prosecution or judicial proceedings. As a result, one state will normally require the assistance of other states in locating offenders, witnesses, evidence and assets through MLA. Since MLA can be conducted during the investigation, prosecution or trial phases of criminal proceedings, the timing of submitting such MLA requests is critical. This chapter provides an overview of when and how MLA requests should be utilised by law enforcement agencies not only during the tracing of the assets but also in order to effectively recover them.

1 Publications of the Basel Institute on Governance:  
 Working Paper No 17: The Role of Donors in the Recovery of Stolen Assets, 2014  
 Emerging Trends in Asset Recovery, 2013  
 Non-State Actors in Asset Recovery, 2011  
 Working Paper No 08: The Recovery of Stolen Assets: Seeking to Balance Fundamental Human Rights at Stake, 2010  
 Recovering Stolen Assets, 2008

To further benefit from profit-generating crime, criminals are usually forced to launder the proceeds to hide the origins thereof. Apart from investigating the crimes that generate the illicit income *per se* and, as criminals try to convert/transform what they have obtained illicitly into ostensibly legitimate assets, a money laundering investigation should take place in parallel. Chapter 5 describes how the international AML framework can be used by practitioners as a tool in the process of tracing illegal assets, depending, of course, on the degree of its implementation in the relevant country's legal system. This chapter seeks to identify the role and use of the various aspects of this framework, such as the use of suppressive and preventive measures, the role of the financial intelligence units and the role of international cooperation, during the process of tracing illegal assets.

The next two chapters of the guide address specific challenges, namely the roles of corporate vehicles and digital currencies in the process of tracing illegal assets.

As corporate vehicles have become an integral and indispensable component of the modern global financial landscape, criminals are constantly misusing them (as well as those who provide trust and company services) to disguise and convert their criminal proceeds before they enter the traditional financial system. The goal of linking the illegally obtained assets to the criminals is becoming increasingly more difficult as the ownership and trail of money and other assets lead away from the crime or the criminal to both domestic and offshore destinations. From this perspective, it is crucial to establish the link between the criminal and the beneficial ownership of such assets. Chapter 6 assists the practitioner in developing an understanding of the types of assistance and structures commonly provided by trust and company service providers (TCSPs) and other professionals being used as the gateway through which criminals disguise the illegal origins of their assets. It will further explain the meaning of 'corporate vehicle' and other related concepts, such as beneficial ownership, the role of TCSPs and trusts, and the most common types of corporate vehicles used for illicit purposes.

As new ways of moving money around the globe have been created, financial transactions, which have always involved cash or cash-derived instruments, now experience new technologies like the Internet, mobile payments and card instruments. Those new instruments will (and already have had) an impact on the effectiveness of existing investigative techniques and best practice to combat financial crimes. The new payment methods that have been developed recently can render previous techniques and best practice obsolete and challenge the way in which financial investigations are conducted. Chapter 7 addresses the new trend of using digital currencies as a means to hide the source of the illicitly obtained proceeds and move them across borders without detection. At the same time, it will present investigative techniques to effectively trace and establish their ownership. Once the veil of secrecy is pierced assets can be sought, found and confiscated, as a digital transaction always leaves a trace.

Finally, we would like to emphasise that all our contributors are practitioners who work for ICAR. They are ready, willing and able to respond to direct requests for assistance from law enforcers around the world and also to requests from anyone with follow-up queries relating to this publication.<sup>2</sup>

---

<sup>2</sup> The Basel Institute on Governance and ICAR have established the Asset Recovery Campus ([www.campus.assetrecovery.org](http://www.campus.assetrecovery.org)), which provides e-learning courses on financial investigations and other topics related to the asset recovery process. It is free of charge for all practitioners tracing and recovering stolen assets. Practitioners can also find more resources and information on asset recovery on our web-based platform: [www.assetrecovery.org](http://www.assetrecovery.org).



# 2. Case strategy and investigation planning

Charles Monteith | Andrew Dornbierer

1. Introduction	25
2. Tracing stolen assets – A multifaceted task	25
3. Setting up an investigation team	26
4. Formulating and initiating the overall case strategy	27
5. Creating an investigation plan	27
5.1 Outlining the features of the offences	28
5.2 Creating an evidence matrix: Outlining the evidence to be gathered and the method to gather it	29
5.3 Outlining a media communication strategy	40
5.4 Outlining case evaluation procedures	41
6. Remember the priority	41
Chapter checklist: Creating an investigation strategy	41





## 1. Introduction

With emphasis firmly placed on identifying, prosecuting and punishing the perpetrators of financial crime, investigators can sometimes lose sight of the need to recover the proceeds of crime. Often there is no asset tracing and little attempt to apply for freezing and confiscation orders. Yet personal enrichment is the main motivating factor for all those engaged in financial crime, and these criminals are generally quite prepared to serve prison time provided they can resume their illegally obtained lifestyles when they come out. Removing the proceeds of crime not only restores the proceeds back to the state or victims, but it also acts as a major disincentive to committing financial crime in the first place. Therefore, the first fundamental priority for law enforcement authorities dealing with such crimes is to **always seek to recover illegally obtained assets**.

Investigators dealing with complex asset recovery cases will generally have to compile and sift through a large amount of information to successfully identify and track proceeds of crime. When investigators are faced with an overwhelming amount of information located in several jurisdictions, it is easy to lose sight of the main purpose of an investigation and to forget this first fundamental priority. It is therefore very important that law enforcement agencies (LEAs) have a well-drafted plan and strategy (which includes the recovery of the proceeds of crime) that will act as a guide and provide a structured method as to how the investigation team will approach the case. Consequently, the second fundamental priority for an investigation team dealing with such cases is to **always have a properly drafted and well-conceived investigation strategy and plan**.

As in most complex asset recovery cases, investigators will find that there will inevitably be assets hidden outside their jurisdiction. The recovery of such assets will require the mutual sharing of information and evidence with the LEAs of these jurisdictions. It is important to remember that you cannot do everything yourself, and, consequently, the third fundamental priority is to **always seek the appropriate assistance**: you will almost always need to seek outside

assistance from foreign investigating agencies through agreements for the exchange of information and through mutual legal assistance (MLA) requests. Such agencies may also be better placed to investigate and prosecute the offences and recover the proceeds of the relevant crimes under their own laws – provided they agree to return these proceeds to the victim country at the conclusion of proceedings (or negotiate an appropriate asset sharing agreement).

This chapter will cover how LEAs can develop effective case strategies that assist in proving essential elements of an offence and increase their ability to successfully identify and track proceeds of crime.

## 2. Tracing stolen assets – A multifaceted task

Asset tracing refers to the process whereby an investigator identifies, tracks and locates proceeds of crime. Investigators trace assets for the purpose of seizing and/or freezing them so that they can be confiscated through a judicial order and, ultimately, returned to the victims of the crime, be that a private party or the state.

In a traditional asset tracing investigation there are three objectives: locating the assets, linking them to an unlawful activity so as to obtain freezing and confiscation orders, and proving the commission of the relevant offences. These should not be considered three distinct and separate steps but rather overlapping objectives that investigators should work towards simultaneously for the purpose of achieving the final goal – to deny criminals the proceeds of their crime.

It is important to note at this point that asset recovery can be achieved through several avenues, the most common of which are conviction-based and non-conviction based forfeiture. In instances of conviction-based forfeiture of assets, a court issues an order for the confiscation of stolen assets after an individual or legal entity has been convicted of a crime. On the other hand, non-conviction based forfeiture

does not require a criminal conviction of an individual or entity but rather enables states to recover illegally obtained assets through direct proceedings against the property itself. This latter avenue is not available in all jurisdictions. Thus, this chapter will focus on asset recovery through a conviction-based approach, though many principles discussed will also apply to a non-conviction based approach.

When following a traditional conviction-based approach to asset recovery, investigations must do more than simply locate the offenders. They also need to acquire sufficient evidence to connect the assets obtained to the unlawful activity so that a judicial order for confiscation can be obtained. Many attempts to recover proceeds of crime fail because of a simple failure to establish such a connection. At the same time, investigators should also try to gather evidence that can be used to prosecute the offender for the underlying criminal activity (or predicate offence) that generated the illicit assets. It is important to stress that a criminal conviction may be followed by the confiscation not only of the assets associated with the specific crime but also of additional assets which the court determines are the proceeds of other similar crimes (under certain conditions).<sup>1</sup>

Increasingly, with the widespread adoption of non-conviction based forfeiture, it is sometimes no longer necessary in many jurisdictions to prosecute an individual to recover proceeds of crime. Enforcement agencies merely seek to recover what appear to be illegal assets or, at very least, assets which cannot be explained. However, the majority of jurisdictions do not yet have non-conviction based forfeiture laws and instead still have to rely on a traditional conviction-based approach to forfeiture.

#### CLASP: THE KEY ELEMENTS OF AN EFFECTIVE MULTIDISCIPLINARY

##### INVESTIGATION TEAM

**Cooperation:** All involved institutions cooperate effectively, fulfill their responsibilities and assist each other efficiently.

**Leadership:** One agency provides clear strategic leadership.

**Allocation:** Roles and responsibilities necessary to fulfill a case strategy are allocated clearly to each agency to prevent the overlap of work and to assist efficiency.

**Sharing:** Relevant information is shared between team members. Good communication is vital to the effective functioning of a team. Team strategy meetings should be held on a regular basis (at least once every three months).

**Proactive approach:** Team members need to be creatively proactive, and should take the initiative rather than waiting for events to unfold.

### 3. Setting up an investigation team

An asset tracing case will require the input of intelligence officers, financial investigators, analysts and lawyers. Therefore, a multidisciplinary team containing each of these skillsets will have to be established as quickly as possible. The investigation will involve a large number of institutions, such as the police, an anti-corruption agency, a financial intelligence unit, a prosecutor's office, a central authority for international assistance requests and possibly an asset recovery office. To cover all the required skillsets, it is important that from the very beginning of an investigation the institutions that will be required to form this multidisciplinary

<sup>1</sup> EU Council Framework Decision 2005/212/JHA of 24 February 2005 on Confiscation of Crime-Related Proceeds, Instrumentalities and Property.

team are identified. Memoranda of Understanding should be drafted and signed between relevant institutions to authorise and legitimise professional relationships and to facilitate cooperation. From these, one institution should be selected to take the lead role in the case investigation. The first strategic consideration is therefore to identify who is best placed to manage the investigation. This lead institution will then assume a proactive role in creating a case strategy and allocating the responsibilities necessary to carry out this strategy to each institution within the team.

A multidisciplinary team can be difficult to manage, and there are several elements that must exist to ensure such a team is effective.

## 4. Formulating and initiating the overall case strategy

When running a multidisciplinary team, the institution acting as team leader must take several actions at the outset. **These actions form the overall case strategy. Namely, the team leader must:**

- Establish the necessary financial and human resources, including ensuring all necessary skillsets are accounted for in the multidisciplinary team and drafting a conclusive budget;
- Set up a tracking and filing and retrieval mechanism for all relevant material that is gathered;
- Establish an investigation plan;
- Map out the tasks and targets of each team member; and
- Explain to each team member his role and responsibilities, and confirm that each team member understands what is expected of him.

As the investigation is carried out, the team leader must also:

- Organise regular team meetings and ensure all operational leads are shared in these meetings; and
- Ensure the investigation plan is updated as the investigation progresses.

## 5. Creating an investigation plan

While all the points of a case strategy are important to the success of an investigation, a critical part of any case strategy is the formulation of an investigation plan. The remainder of this chapter will focus on creating an effective and solid investigation plan that can facilitate and direct an investigation.

Investigations are always unique. The amount and type of information available to an agency during the early stages of an investigation very much determines how a particular investigation will be conducted from the outset. Consequently, the strategic approach to all investigations should be evidenced through a clear investigation plan.

The aim of an investigation from the start should be the transformation of relevant intelligence into admissible evidence that can be used to convict the suspects and recover stolen assets. An investigation plan is a drafted outline of the overall case strategy that will be adopted to achieve this aim. It effectively serves as the guide to the overall case strategy. It is important to remember that the plan must take the form of a living document – meaning it must be revised and updated throughout an investigation so that it accurately reflects the evidence gathered at various stages, the developments in the case and the evolving understanding of the case.

The investigative plan should cover and include the following:

- An outline of the features of the predicate offence(s), including the proceeds of crime/illegal assets generated from these offences (if these have already

been identified) and an outline of the potential money laundering offences that may stem from these original predicate offences;

- An outline of the relevant evidence required to establish the offences and demonstrate the proceeds of crime generated and an outline of the investigation powers and tools to be adopted to gather such evidence (the evidence matrix);
- A media communication strategy; and
- An outline of procedures to allow for the ongoing evaluation of the investigation.

This chapter will now go through each of these above items in turn and explain in greater detail what the investigation plan needs to cover under each issue.

## 5.1 Outlining the features of the offences

### 5.1.1 The predicate offence

Proceeds of crime derive from a criminal offence. Consequently, in order to obtain a freezing order, and ultimately a confiscation order, it is vital to link the proceeds to a predicate criminal offence. Therefore, an important element of any asset recovery case will be clearly outlining the facts surrounding the commission of the original predicate offence and the illegal proceeds it generated. Outlining the facts will also assist investigators when drafting the evidence matrix (see subsection 2 below). However, it is important to remember that there will be a constant need to review and update the investigative plan as the facts available to investigators will change as the investigation progresses (particularly after the early stages).

When outlining the facts of the original offence, investigators should aim to answer the following questions:

**WHO** are the subjects of the investigation? Identify all the individuals and businesses related to the criminal activity

and their relationship to each other.

**WHAT** was the offence that took place? Identify the specific laws that may have been violated. What proceeds of crime were generated and what happened to them?

**WHERE** was the criminal act committed? Identify all the locations where the parties to an offence committed the actions that amounted to the offence (for example, where meetings took place or where money was exchanged). Where are the proceeds of crime currently being held? These facts are important in assessing issues of jurisdiction.

**WHEN** did the actions that constitute the crime take place? Identify all the times and dates that the relevant actions took place. This will be particularly relevant when assessing the statutory limitations on pursuing actions.

**WHY** did the criminal parties commit the actions? Identify the motivation for the actions.

**HOW** did the criminal parties commit the crime? Investigators should place all the relevant events and actions in sequence to identify the method used by the criminals to commit the crime and generate the proceeds of crime.

### 5.1.2 Outlining the features of the money laundering offence

If a crime has generated proceeds, and these proceeds have in turn been transferred and transformed by a party with the intention of disguising their illicit origin, then generally a money laundering offence will also have been committed. While establishing the features of the predicate offence (outlined above), investigators should also look to establish the features of any consequent money laundering offence (see chapter 4) and aim to answer the same questions that apply to the original offence accordingly, namely:

**WHO** are the subjects of the money laundering investigation? Identify all the individuals and businesses that were involved in the laundering and their relationship to each other.

**WHAT** was the offence that took place and what were the proceeds of crime generated? Identify the specific money laundering offence that has been committed with a reference to law, and identify the form and amount of the proceeds of crime that were generated.

**WHERE** was the money laundering offence committed? Identify all the locations where the parties to an offence committed the actions that amounted to the offence. In the case of money laundering, these locations will most likely be spread across several jurisdictions and will probably involve additional money laundering offences under each jurisdiction.

**WHEN** did the laundering take place? Identify all the times and dates that the relevant actions took place. This will be particularly relevant when assessing the statutory limitations on pursuing actions.

**WHY** did the criminal parties commit the actions? Identify the motivation for the actions. (In money laundering the motivation could range from simply wanting to disguise funds to funding terrorism or other organised criminal actions.)

**HOW** did the criminal parties launder the proceeds? Investigators should place all the relevant events and actions in sequence to identify the method used by the criminals to launder the proceeds of crime.

## 5.2 Creating an evidence matrix: Outlining the evidence to be gathered and the method to gather it

Investigators will need a significant amount of admissible evidence to establish the facts surrounding and proving each element of an offence. Consequently, determining what evidence is required to establish an offence is an essential part of strategic planning.

In mapping out exactly what evidence should be gathered, investigators should refer to the outlines of both the predicate and money laundering offences that have been drafted according to the above sections. Then, ask what

evidence is needed to persuade a court that the subject of the investigation has committed the outlined crimes. **Evidence required in order to link illegal assets to the offences will also have to be obtained - often both to convict the perpetrator and also to trace/recover the assets. Thought should be given to what is required to obtain early freezing orders at home and/or abroad.**

An analysis of the evidence required to prove the offence allows the investigation team to identify any gaps in the evidence gathered to date and thus to focus on acquiring any further relevant evidence from appropriate sources.

Some agencies draft an outline of the evidence gathered (an evidence matrix), which sets out an evidence trail. An evidence matrix is a useful reference throughout the course of the investigation to determine whether the evidence obtained would be admissible and likely to withstand judicial scrutiny.

When filling out the evidence matrix, investigators will have to outline four important things:

1. The elements of the offence that need to be proven;
2. The facts that need to be established to prove each element;
3. The type of evidence that should be gathered to establish each of these facts; and
4. The method that should be used to gather this evidence.

Take, for example, a case where investigators have received intelligence that a senior public official in the resources ministry of Country X, Mr Smith, illegally transferred USD 100,000 from his ministry's 'oil revenue' bank account (of which he is an authorised signatory) to an offshore bank account in Country Y (of which he is a beneficial owner). Investigators have also received intelligence that Mr Smith used this same money to then purchase a house in Country Y.

To add to the example, Country X has a very straightforward section in its criminal code for embezzlement which states: 'If a public official transfers or converts public funds, without authority, for the purpose of altering the ownership of these funds for the benefit of himself or a third person, he or she is guilty of a crime'.

Using the above example of Mr Smith, the following paragraphs will go through each of the four sections to an evidence matrix and will provide an updated example of a single matrix as each section is drafted.

### 5.2.1 Outlining the elements to be proven

A matrix should be drawn up for each offence that needs to be established. When outlining the elements of an offence to be proven, the investigator will need to break down the legislative provisions piece by piece. An element is essentially a point of fact that an investigator must demonstrate happened. If an investigator was to begin drafting an evidence matrix for the example of Mr Smith with the idea of establishing an offence of embezzlement according to the provision above, the matrix may initially look something like this:

#### Offence: Embezzlement

Elements of offence	Facts to prove each element	Type of evidence to be gathered to prove facts	Method to use to gather evidence
1. Mr Smith is a public official.			
2. Mr Smith transferred or converted public funds.			
3. Mr Smith did so without authority.			
4. Mr Smith did so with the intention of altering the ownership of the property for his benefit.			

Remember to include all potential offences when drafting matrices in an asset recovery case, including money laundering (for the purposes of simplicity, however, we are including just the predicate offence of embezzlement in the example).

### 5.2.2 Outlining the facts to prove each element

The next step for an investigator will be to outline each of the facts that must be proven to establish each element. For example, referring to the case of Mr Smith, the first element is 'Mr Smith is a public official'. Consequently, to prove this element, an investigator will have to establish the fact that 'Mr Smith is an employee of the resources ministry'.

When drafting this section, an investigator should refer to his outline of the 'features of the offence' (see the section on 'Outlining the features of the offence') where he should have already drafted preliminary answers to the questions 'Who? What? Where? When? Why? How?' based on the intelligence that has already been received. The answers to these questions, and the facts they demonstrate, may prove to be very useful in establishing the elements of the crime. These facts should be slotted into the evidence matrix where relevant. For instance, based on the intelligence already available in the case of Mr Smith, an investigator would be able to answer the 'Where?' question (as in 'Where were the criminal acts committed?'), as he is already aware that 'Mr Smith transferred funds from County X to Country Y'. Consequently, this answer could be used as a fact to prove the second element of the offence, 'Mr Smith transferred or converted public funds'.

If an investigator were to continue drafting the evidence matrix by listing all the relevant facts, it may look something like this:

## Offence: Embezzlement

Elements of offence	Facts to prove each element	Type of evidence to be gathered to prove facts	Method to use to gather evidence
1. Mr Smith is a public official.	<ul style="list-style-type: none"> <li>Mr Smith is employed as a high-ranking public official in the resources ministry.</li> </ul>		
2. Mr Smith transferred or converted public funds.	<ul style="list-style-type: none"> <li>Mr Smith had authority over the oil revenue account.</li> <li>Mr Smith authorised the transfer of USD 100,000 from the account in Country X to a third party account in Country Y.</li> </ul>		
3. Mr Smith did so without authority.	<ul style="list-style-type: none"> <li>There was no authority from the resources ministry to transfer USD 100,000.</li> <li>No contract or project existed within the ministry that required the transfer of USD 100,000.</li> <li>No benefit was received by the ministry in consideration of USD 100,000.</li> </ul>		
4. Mr Smith did so with the intention of altering the ownership of the property for his benefit.	<ul style="list-style-type: none"> <li>Mr Smith transferred funds to his own private account. Mr Smith then used these funds to purchase a property. The property was purchased in his own name.</li> </ul>		



### 5.2.3 Outlining the type of evidence to be gathered to prove the facts

The next step for an investigator will be to outline the specific types of evidence that will be required to establish each of these facts outlined in the above section.

The evidence itself will depend on the type of crimes under investigation, but in most asset recovery cases the type of evidence required frequently includes:

- Communication records (including telephone, hard copy and Internet communications);
- Statements and depositions of the subjects of investigation and of witnesses;
- Banking and financial documents (such as account statements, account opening information and supporting documents, institution drafted risk assessments and due diligence reports, and suspicious activity reports);
- Corporate registry documents, such as registration and share certificate documentation;
- Land registry documents (such as certificate of title);
- Business contracts; and
- Legal instruments (such as trust documents [see chapter 6]).

It is important to remember that the required evidence needed will vary greatly from case to case. Take, for example, a case of bribery – in such cases a bribe is often disguised in the form of payments for children's school fees or property given to children, parents or siblings, or even obscurely linked individuals, such as gardeners or other employees. All transfers of property in this regard will need thorough evidencing.

Returning to the example of Mr Smith, if an investigator needed to prove that 'Mr Smith is employed as a high-ranking public official in the resources ministry', then one thing that might be required is Mr Smith's employment contract. As another example, if an investigator needed to prove that 'Mr Smith authorised the transfer of USD 100,000 to a third party account', then the investigator may need to acquire the instructions from Mr Smith that gave permission to the bank to make the transfer.

At this stage, the evidence matrix may start to look a bit like this (see next page):

## Offence: Embezzlement

Elements of offence	Facts to prove each element	Type of evidence to be gathered to prove facts	Method to use to gather evidence
1. Mr Smith is a public official.	<ul style="list-style-type: none"> <li>Mr Smith is employed as a high-ranking public official in the resources ministry.</li> </ul>	<ul style="list-style-type: none"> <li>Employment contract</li> </ul>	
2. Mr Smith transferred or converted public funds.	<ul style="list-style-type: none"> <li>Mr Smith had authority over the oil revenue account.</li> <li>Mr Smith authorised the transfer of USD 100,000 from the account in Country X to a third party account in Country Y.</li> </ul>	<ul style="list-style-type: none"> <li>Bank account documents indicating Mr Smith is a signatory of the account</li> <li>Transfer instructions received by the bank from Mr Smith</li> </ul>	
3. Mr Smith did so without authority.	<ul style="list-style-type: none"> <li>There was no authority from the resources ministry to transfer USD 100,000.</li> <li>No contract or project existed within the ministry that required the transfer of USD 100,000.</li> <li>No benefit was received by the ministry in consideration of USD 100,000.</li> </ul>	<ul style="list-style-type: none"> <li>Confirmation from the resources ministry stating no authorisation was given for the transfer</li> <li>Resource ministry financial statements that confirm that no benefit had been received by the ministry in return for transferring the money</li> <li>Documentation (such as legislation or ministry regulations) outlining the function and responsibilities of Mr Smith</li> <li>Witness statements from fellow employees who would normally have the authority to transfer money confirming they did not give authorisation</li> </ul>	

4. Mr Smith did so with the intention of altering the ownership of the property for his benefit.

- Mr Smith transferred funds to his own private account.
- Mr Smith then used these funds to purchase a property.
- The property was purchased in his own name.

- Bank account statements indicating Mr Smith's account received funds
- Documentation from the land registry demonstrating ownership of property transferred to Mr Smith
- Copy of the contract of sale of the property outlining the method of payment
- Bank account statements demonstrating transfer of money to previous owner of property
- Oral testimony of the estate agent/property conveyancer/corporate service provider who facilitated the transfer of property

#### 5.2.4 Outlining the investigation powers, tools and sources to be used to gather the evidence

The success of an investigation often depends largely on the investigating authority's ability to utilise all the powers, tools and sources available to it to gather evidence and trace assets. In this stage, investigators will need to aim at converting intelligence that they gather into admissible evidence that can be used in court proceedings. In doing so, they must consider the reliability of sources and the relevance of the information received in regards to its ability to establish facts relevant to proving the elements of an offence.

The types of powers, tools and sources available vary in nature and can include specialised investigating agencies, such as Financial Intelligence Units (FIUs), different sources of intelligence as well as strategies of cooperation with foreign enforcement agencies. Some of these are outlined below in more detail.

##### *Financial intelligence and FIUs*

When assets flow through the financial system, the transfer of funds in and out of accounts usually leaves an audit trail, which can be tracked and detected. Financial intelligence refers to any data that can be obtained to assist in this process and that can ultimately be used to create a financial profile of a suspect (see chapter 3). This data can emanate from a wide range of sources and can include information obtained

from financial institutions (such as account statements, opening account information and suspicious activity reports), government agencies, e-banking facilities, money service providers, law and accounting firms, real estate agents, trust and corporate service providers, and business competitors.

To assist with collating such data, FIUs have been established in most jurisdictions around the world. Primarily, they receive, analyse and disclose information provided by financial and non-banking financial institutions relating to suspicious or unusual financial transactions, but they also build up profiles of individuals and money laundering techniques. Furthermore, in 1995, the Egmont Group of Financial Intelligence Units (Egmont Group) was created, which provides a forum for FIUs of different states to share financial intelligence relevant to suspects investigated in different jurisdictions, greatly speeding up international coordination.

For instance, in our case example, financial intelligence can be obtained that establishes the final form and location of the USD 100,000 embezzled by Mr Smith. Specifically, the FIU in Country X can be asked to contact the FIU of Country Y and informally inquire about the existence of any bank accounts belonging to Mr Smith, his companies or his family members in Country Y. They could also ask the FIU in Country Y to investigate whether any major property purchases have been made relating to Mr Smith. In response, Country Y may provide intelligence that can assist the investigation in Country X. It is important to note, however, that this information can only be used for intelligence purposes. If the enforcement agencies in Country X subsequently decide to use information obtained from Country Y as evidence in court proceedings in Country X, they will need to first send a formal MLA request for the evidence and receive copies of this evidence through official channels (for more information see the below section on 'Cooperation with foreign law enforcement agencies' as well as chapter 4 on Mutual Legal Assistance).

Chapter 5 provides additional information and an overview of different types of FIUs and how the anti-money laundering (AML) framework can be utilised for tracing illicit assets.

#### *Voluntary human intelligence*

Human intelligence sources remain one of the key intelligence tools for LEAs, particularly when dealing with money laundering networks that are very difficult to penetrate. Voluntary human intelligence encompasses all instances in which an individual comes forward and provides information that can assist in the investigation and generally refers to informants, whistle-blowers, victims or disgruntled co-conspirators. The information provided by such intelligence can be critical to a successful investigation, as it can provide inside information into criminal networks as well as new directional leads, which may result in the gathering of further incriminating evidence.

While the information provided by such individuals can be invaluable, it is important to exercise a considerable level of caution, particularly when evaluating the motives of the individual providing such information, as misleading or wrong information can compromise and taint an entire investigation.

To apply this to the example of the corrupt public official above, human intelligence may take the form of a whistle-blower in the official's ministry who also has access to the relevant bank account and who is aware of the location to which the stolen funds may have been transferred. Nevertheless, it is important to remember that with all such human intelligence sources, investigators must take care to verify the integrity of any information that is offered so as to rule out any chance that the information may taint the investigation.

#### *Compulsory interviews*

In some circumstances, and when an investigative agency has such powers, it may be necessary or desirable to compel individuals to attend a compulsory interview. Compulsory interviews are usually necessary when:

- An interview must be conducted quickly because of time constraints;
- An individual concerned with the investigation is willing to speak with the agency but wants to be compelled to do so in order that he or she is not seen as voluntarily providing information;

- An individual has a contractual or other legally binding confidentiality obligation, and compulsion is required to override that obligation;
- An individual refuses to consent to a voluntary interview or tries to stipulate conditions that are not acceptable (such as a privilege against self-incrimination);
- An investigator suspects the interviewee may not be truthful in a voluntary interview; and
- An investigator wishes to confront the interviewee with a more formal environment to reinforce the need to give truthful accounts.

Compulsory interviews have their drawbacks, however, and it is important to remember that what is said in a compulsory interview may not be admissible against the main suspects (depending on local criminal procedure laws). Also, they cannot be used to self-incriminate unless a caution is given. Furthermore, anything said by investigators in an interview may alert the suspect to any covert investigative actions that may be ongoing. Consequently, the timing of such an interview must be carefully considered. Also, always remember to independently verify anything said in such interviews.

#### *Compulsory requests for information*

Compulsory requests for information can result in the production of valuable information. Agencies should first identify the parties to which it is appropriate to issue a request for information and thereafter draft the request accordingly. Compulsory information requests should not be utilised when there is a risk of destruction of or interference with information. Remember, however, to keep requests as succinct and simple as possible because unnecessarily broad requests for information may cause investigational delays due to the time required to respond. In our example of Mr Smith, a compulsory request for information could be issued to the bank for relevant banking documents or to the ministry for relevant employment information. Or, furthermore, such a request could be

made to Mr Smith's telephone providers to produce Mr Smith's communications, such as messages and emails.

#### *Physical surveillance and observation*

Physical surveillance is a traditional and excellent source of intelligence. Physically observing a suspect can give investigators an idea of the individuals the suspect meets on a day-to-day basis and the networks in which he or she is involved. Furthermore, it may reveal the places that the suspect visits and the location of properties and companies controlled by the suspect of which investigators were previously unaware.

#### *Searches and seizures*

Searches can be a very effective method of gathering evidence. They minimise the opportunity for document destruction and concealment, and they can avoid deliberate or inadvertent failure to produce documents following an agency request. The downfall of conducting searches and seizures is that the amount of material gathered during an operation is sometimes very large, which is consequently time-consuming to analyse.

#### *Open sources of intelligence*

Open source intelligence has become increasingly utilised in the past decade, and it involves the acquisition and analysis of information from publicly available sources. For instance, due to the exponential growth of the Internet, an increasing number of sources are becoming publicly available providing investigators with a rich source of high quality evidence that can be used to support strategic and operational decisions. Examples of such sources include online media (newspapers, blogs, etc.), directories, government reports and documents (including asset declaration forms), statistical databases and publicly available databases (such as property and corporate databases), which can all be easily located using publicly available search engines, such as Google, or analysed using specifically tailored programmes, such as the International Centre for Asset Recovery (ICAR) Asset Recovery Intelligence System (ARIS) tool.

An online open source that has been of particular use to investigators in recent years is social media. Facebook and LinkedIn, for instance, have become rich sources of

information, as they can provide a detailed insight into an individual's contacts and movements and, on some occasions, their major purchases. In returning to the example of our corrupt public official, an investigator may be able to acquire a great deal of valuable information by examining the Facebook profile of this public official, or if he does not have one, the profile of his wife, children or known contacts. During the course of such analysis, investigators may discover photos of holidays that this public official has taken with his family, including pictures displaying assets such as recently purchased holiday homes or luxury yachts. The location of such pictures will further indicate the jurisdictions in which these assets could be found and seized.

#### *Cooperation with foreign enforcement agencies*

When assets are situated in foreign jurisdictions, enforcement agencies can cooperate with foreign counterparts both to obtain information and evidence pertaining to the location of assets and to actually have the assets frozen and seized.

For instance, as it appears our corrupt official has transferred his criminally obtained assets from a bank account in Country X to an account in Country Y, cooperation will be needed from the enforcement agencies in Country Y to investigate the trail of the assets and to establish their current location. Assuming that Mr Smith bought a house in Country Y with the assets, cooperation will also be needed from Country Y to freeze such assets and prevent them from being sold.

In initially tracing the path of the assets, the investigators in Country X could informally exchange information with the enforcement agencies from Country Y. For instance, if both countries have an FIU that is a member of the Egmont Group, they can utilise this network and its mechanisms to allow for the informal and rapid exchange of information regarding the suspicious assets (as mentioned above). Alternatively, if each state is a member of an international inter-agency law enforcement network, such as the Camden Assets Recovery Interagency Network (CARIN) or the Asset Recovery Inter-Agency Network of Southern Africa (ARINSA), they could also utilise these networks to informally share and receive information. This will allow Country Y to quickly inform

Country X of any asset movements that may have taken place.

However, in order to seize the suspicious assets, Country X will need to ask Country Y to do so through a request for MLA. MLA is a means for one jurisdiction to formally provide assistance to competent authorities (such as prosecutors, magistrates and even law enforcement agents) in another jurisdiction so that the former may have certain investigatory or judicial acts (such as service of process, evidence or seizure of assets) recognised, processed and carried out in the latter as the authorities of the requesting jurisdiction do not have the legal standing to enforce them in the requested jurisdiction (for more information see chapter 4 on Mutual Legal Assistance). Thus, if prosecutors in Country X wish to use evidence (such as bank statements) located in Country Y in criminal proceedings in Country X against the public official, they will also need to extract this evidence through a formal request for MLA in order to ensure that this evidence is admissible during legal proceedings.

Returning to the evidence matrix, if an investigator takes into account these sources and methods for gathering evidence, he should be able to list strategies to obtain the specific evidence he needs to gather to prove the facts of the case. At this stage, an investigator's evidence matrix may look like this:

## Offence: Embezzlement

Elements of offence	Facts to prove each element	Type of evidence to be gathered to prove facts	Method to use to gather evidence
1. Mr Smith is a public official.	<ul style="list-style-type: none"> <li>Mr Smith is employed as a high-ranking public official in the resources ministry.</li> </ul>	<ul style="list-style-type: none"> <li>Employment contract</li> </ul>	<ul style="list-style-type: none"> <li>Compulsory request for information directed to ministry (if necessary)</li> </ul>
2. Mr Smith transferred or converted public funds.	<ul style="list-style-type: none"> <li>Mr Smith had authority over the oil revenue account.</li> <li>Mr Smith authorised the transfer of USD 100,000 from the account in Country X to a third party account in Country Y.</li> </ul>	<ul style="list-style-type: none"> <li>Bank account documents indicating Mr Smith is a signatory of the account</li> <li>Transfer instructions received by the bank from Mr Smith</li> </ul>	<ul style="list-style-type: none"> <li>Compulsory request for information directed to bank and /or production order obtained</li> <li>Compulsory request for information directed to bank</li> </ul>
3. Mr Smith did so without authority.	<ul style="list-style-type: none"> <li>There was no authority from the resources ministry to transfer USD 100,000.</li> <li>No contract or project existed within the ministry that required the transfer of USD 100,000.</li> <li>No benefit was received by the ministry in consideration of USD 100,000.</li> </ul>	<ul style="list-style-type: none"> <li>Confirmation from the resources ministry stating no authorisation was given for the transfer</li> <li>Resource ministry financial statements that confirm that no benefit had been received by the ministry in return for transferring the money</li> <li>Documentation (such as legislation or ministry regulations) outlining the function and responsibilities of Mr Smith</li> <li>Witness statements from fellow employees who would normally have the authority to transfer money confirming they did not give authorisation</li> </ul>	<ul style="list-style-type: none"> <li>Subpoena witnesses</li> <li>Conduct searches</li> <li>Compel the handing over of documents</li> <li>Expert witnesses (such as independent accounting specialists to analyse ministry accounts)</li> </ul>

<p>4. Mr Smith did so with the intention of altering the ownership of the property for his benefit.</p>	<ul style="list-style-type: none"> <li>• Mr Smith transferred funds to his own private account.</li> <li>• Mr Smith then used these funds to purchase a property.</li> <li>• The property was purchased in his own name.</li> </ul>	<ul style="list-style-type: none"> <li>• Bank account statements indicating Mr Smith's account received funds</li> <li>• Documentation from the land registry demonstrating ownership of property transferred to Mr Smith</li> <li>• Copy of the contract of sale of the property outlining the method of payment</li> <li>• Bank account statements demonstrating transfer of money to previous owner of property</li> <li>• Oral testimony of the estate agent/property conveyancer/corporate service provider who facilitated the transfer of property</li> </ul>	<ul style="list-style-type: none"> <li>• Informal inquiry with Country Y FIU to obtain bank account and property ownership transfer information</li> <li>• MLA request to Country Y to obtain bank account transfer information, property ownership transfer information</li> <li>• Interviews with witnesses (possibly requested through MLA request to Country Y depending on location of witnesses)</li> </ul>
---	---	--	---

### 5.3 Outlining a media communication strategy

When creating an investigation plan, it is important that investigators draft and agree on a media communication strategy. Asset recovery cases can often attract a high level of media attention, and it is important that all members of the investigation team understand what can and should be conveyed during each stage of an ongoing investigation.

One of the key issues in asset recovery is that the public does not fully comprehend the legal processes that have to be undertaken before any assets can be recovered. Hence, agencies often have to deal with unrealistic expectations from the public. It is best to address expectations right at the beginning of an investigation (when it can safely be made public) and stress that the recovery of illegally

obtained assets has to follow the due process of law (and court decisions) both in the country where the corruption occurred and in the country where the assets are located. Investigators should stress that all of this can be a time-consuming process unless the suspects agree to return the assets or a settlement is reached. This is also true of the assets of sanctioned individuals or entities.

Whilst it may not be possible to confirm or deny that an investigation has commenced, once elements of the investigation become public (that is, after searches, seizures, arrests take place) it is important to engage with the wider public as much as possible.



## 5.4 Outlining case evaluation procedures

Throughout the course of the investigation, it is good practice to revise and adapt the investigation plan and strategy to reflect the evidence as it is obtained and also to evaluate the relevant issues, to consider emerging issues, to assess evidence-gathering strategies, to monitor and re-set objectives, and to redistribute administrative tasks. Therefore, it is important that a process for evaluation is also included in the investigation plan, which outlines the method and timeframe for a continuous review of the case at hand.

This evaluation process should indicate a timeframe for periodic team meetings, which are an effective way to ensure that the investigative plan is kept up-to-date and incorporates all relevant issues. In addition to team meetings, agencies should hold more formal internal meetings periodically to update senior staff and decision-makers on the progress of the investigation at critical stages when decisions need to be made. Agency staff may prepare papers that set out updates and proof issues and case agendas for presentation and distribution at such meetings.

## 6. Remember the priority

Once an investigation plan and strategy is in place, investigators must put it into action. In doing so, it is very important that investigators keep the priority of the investigation in the back of their minds at all times: to recover the proceeds of the crime. All efforts need to be directed towards achieving this aim. This means that investigators must:

1. Identify the assets that have been stolen;
2. Trace the assets to their current location;
3. Link the asset to their criminal source by gathering sufficient evidence; and
4. Use this evidence to obtain the necessary orders to freeze, seize and confiscate the assets.

### CHAPTER CHECKLIST: CREATING AN INVESTIGATION STRATEGY

- Set up a multidisciplinary investigation team drawing on all the relevant agencies and establish which agency will take the lead role.
- Outline the known facts of the original offence and the money laundering offence with reference to the questions: Who? What? Where? When? How?
- Draft an evidence matrix which outlines:
  - The elements of the offence that needs to be proven with reference to the relevant criminal statute;
  - The facts that need to be established to prove each element of the offences;
  - The type of evidence that should be gathered to establish each of these facts; and
  - The method or source of this evidence.
- Outline a media communication strategy.
- Outline a procedure for the ongoing evaluation of the case.
- Remember the priority of the case: trace, freeze, seize and **confiscate the assets**.



# 3. Financial profiling

Federico Paesano

- 1. Introduction **45**
  - 1.1 A tool to provide indirect or circumstantial evidence **45**
  - 1.2 A tool to prove the crime of 'unexplained wealth' or 'illicit enrichment' **46**
- 2. Source and Application of Funds analysis to evaluate unexplained income **46**



## 1. Introduction

As presented in detail in chapter 2 of this guide, the first step towards the recovery of stolen assets is a full financial investigation that identifies the assets and follows the trail back to their origin. During this process, financial profiling is a strong tool that can help practitioners to establish the link between criminals, their illicit activities and their illicitly obtained assets.

The most common and easiest method of both financial profiling and proving unknown income that may be illegal is the 'Source and Application of Funds' analysis, also known as the 'expenditure', 'funds flow' or 'application of funds' method. During a defined period of time, the Source and Application of Funds method compares the expenditures of a person with his legal and known income. The proceeds of a criminal activity will be kept in cash or in a bank account and are used to buy assets, pay off debts or finance personal expenses. The following method takes all these means into account.

This tool can be used to provide circumstantial evidence for the commission of a crime but it can also supply direct evidence in jurisdictions where 'unexplained wealth' or 'illicit enrichment' is criminalised as a stand-alone offence.

### 1.1 A tool to provide indirect or circumstantial evidence

During an investigation, the best case scenario is one in which the investigator has direct evidence of the commission of the crime: a bribe paid directly into the public official's bank account, a video recording that documents the illegal action or an arrest of the perpetrator in an undercover operation as he receives the bribe money. This kind of evidence, though very strong when brought before the court, is becoming increasingly hard to find. New technologies and payment methods, like digital currencies, allow criminals to transfer funds and pay bribes without moving from their desks and sometimes without ever meeting each other. In addition, corrupt officials and money launderers often have

on their payrolls skilled accountants and lawyers who assist them in creating complex financial structures to hide the true ownership of money. Last, but not least, in corruption offences both parties – i.e. the briber (the person giving the bribe) and the bribee (the person receiving the bribe) – benefit from the crime, which is often committed behind closed doors, and they have no interest in reporting it. As a result, the investigation often commences months after the commission of the unlawful activity making the chances of finding direct evidence almost impossible.

How can this veil of confusion and secrecy be lifted? The answer is to follow the money and seek the beneficial owner of the illegal assets – the person driving expensive cars and living in luxury vacation properties.

Therefore, the investigator is often left with only the possibility of using an indirect method of proof to prove his case, i.e. the use of circumstantial evidence to prove the commission of a crime. Indirect methods can be used when the suspect received currency or other payments or assets that cannot be directly traced, and they are based on the assumption that the proceeds of crime in any significant amount will eventually show up, directly or indirectly, in the perpetrator's accounts, assets or expenditures.

During medieval times, the common law tradition viewed the 'eyewitness testimony paradigm' as the only reliable form of evidence. As a result, circumstantial evidence is often considered to be less reliable and is therefore used more reluctantly. In the past, however, corruption in all its facets was not understood and was not as endemic as it is in our society. Centuries have passed but the mind-set remains unchanged. Emphasis and reliance is placed on direct evidence as opposed to circumstantial evidence despite the fact that reality demonstrates the limitations of the 'eyewitness testimony paradigm' in successfully prosecuting corruption cases.<sup>1</sup> Thus, a shift to the use of indirect methods to prove the illicit conduct is very important and valuable.

<sup>1</sup> E. Hoseah, *Corruption in Tanzania: The Case for Circumstantial Evidence*, Amherst, NY, Cambria, 2008.

The Source and Application of Funds method in this instance provides indirect evidence, and it is used in the course of an investigation when the following circumstances are met:

- Direct evidence is not available.
- During a defined period of time, the suspect spent or used in other ways far more money than he had legally available.

### 1.2 A tool to prove the crime of 'unexplained wealth' or 'illicit enrichment'

In jurisdictions where 'unexplained wealth' or 'illicit enrichment' is a stand-alone offence, the investigator needs to prove the extent of the suspect's illicit wealth. He needs to establish that the difference between the suspect's expenditures and his legal income must have been derived from illicit activities and is therefore subject to confiscation. In order to prove this, the investigator can apply the Source and Application of Funds method as described below.

This powerful legal provision may not be available in many countries as some consider the crime of unexplained wealth to involve a reversal of the burden of proof, which is contrary to their constitutions and the fundamental principles of their legal systems. The perpetrator no longer enjoys the fundamental right to be presumed innocent until proven guilty as he is required to prove the legal source of his wealth. In a scenario where the suspect, a public official for instance, allegedly received bribes for contracts he awarded illegally, this method alone does not prove the crime per se but demonstrates that the person was spending money far above his legal means. Some countries may require the investigation to establish evidence that indicates that the subject committed a criminal offence (bribery or abuse of office in the example above) in order to link his illicit activity to the unexplained wealth. In this case, the Source and Application of Funds analysis provides corroborating evidence. Evidence secured as a result of the Source and Application of Funds analysis will complement the testimony

of witnesses and research into any other possible origin of the unexplained wealth in order to enable the court to come to the conclusion that the funds must have emanated from illicit activity.

Therefore, the Source and Application of Funds method can be used differently depending on the legal system of the country where the investigation is conducted.

## 2. Source and Application of Funds analysis to evaluate unexplained income

This method compares the money spent, saved and used in any manner to the known and legal income that the person earned during a set time period. 'Known and legal' means that each and every source of money included in the calculation must have a legal and documented origin.

This concept expressed in a formula would appear as follows:

FOR A SET PERIOD OF TIME, THE SUSPECT HAD:	
Total expenditures and other applications of money:	3,000,000 EUR
Minus total known and legal sources of income:	100,000 EUR
Equals illegal or unexplained income:	2,900,000 EUR

A Source and Application of Funds analysis will compare every financial transaction made by the suspect during a set period of time. This period can be a calendar year (1 January to 31 December) or any other timeframe that will show an increase in spending or wealth far above the legal means of the subject and that includes the period in which he allegedly committed the illicit activity. When dealing with a public corruption case in which a 'wealth declaration' is mandatory by law, a good starting point for this timeframe could be the date on which the allegedly bribed official filed the statement. By using the data included in a

document compiled or presented by the suspect himself, the investigator will avoid any possible denial by the defence.

The chart below is a simple example of a completed Source and Application of Funds analysis.

The source column will show the balance of every account at the beginning of the period under consideration. Similarly, the application column will be filled with the balance of the same accounts at the end of the timeframe. The next step is to list every legal and known source of income (left column) and all the applications (right column). The first lines

of each of the two columns (sources and applications) are filled with data taken from every bank account controlled by the individual under scrutiny and, if available, his wealth and/or tax declaration. What about cash? Apart from cash declared in an official document, cash deposits into the suspect's bank accounts will not be considered 'legal and known' sources of money, unless he is capable of explaining and documenting their origin.

Typical **sources of funds** include salary, gifts (the investigator will identify the real nature of these gifts by interviewing people who allegedly made them), rental income, dividends,

Period = 01/01/2014 - 30/06/2015			
Sources		Applications	
Item	Amount	Item	Amount
Opening Balance - Tashi Bank	2'500.00	Closing Balance - Tashi Bank	128'904.00
Opening Balance - Carribean Trust Bank	0.00	Closing Balance - Carribean Trust Bank	410'000.00
Opening Balance - Punjab National Bank	0.00	Closing Balance - Punjab National Bank	440'000.00
Cash declared	1'000.00		
Salary from Government	216'600.00	University London	72'000.00
		Loan	37'800.00
		Spa	3'990.00
		Apartment rented in London	23'945.00
		Restaurants	13'500.00
		Telephone and electricity	9'683.00
		Mercedes	87'000.00
		Apartment Cayman	300'000.00
		House renovation	125'000.00
<b>Total legal and known sources</b>	<b>220'100.00</b>	<b>Total applications</b>	<b>1'651'822.00</b>
		<b>MINUS legal and known sources</b>	<b>220'100.00</b>
		<b>Illegal/unknown income</b>	<b>1'431'722.00</b>

cash on hand legally declared (for example, in a wealth declaration), sale of properties occurring within the period, inheritances (if documented), insurance proceeds, disability payments, gambling winnings.<sup>2</sup> What about the revaluation of a piece of land, a house, a precious painting or anything with an appreciating (or depreciating) value? A change in the fair market value of an asset does not indicate a source or application of funds, because the increase or decrease in the value of the property would not represent a receipt or expenditure of cash or a cash equivalent. Market price is a hypothetical value that does not create any financial flow until the item is sold and is therefore left outside the calculation.

Typical **applications** include rental of properties, payments for mortgages, cars, real estate properties, boats and airplanes (including their maintenance), credit card payments, clothes, food, utilities, travel, shares, insurance. Is there a way in which cash can be considered an application? If during a search at the suspect's house or in any other place under his control cash is found and seized (because there are grounds to believe it is the proceeds of a crime), then the cash can be considered an application in the Source and Application of Funds method.

---

2 Gambling winnings must come from a documented source before they can be taken into account. However, this may not be sufficient. Large sums or a series of smaller amounts must be placed under intense scrutiny and further investigation since they might be the result of a money laundering scheme.







# 4. Mutual legal assistance

Pedro Gomes Pereira

1. Introduction	53
2. Step 1: Preparing for mutual legal assistance (MLA)	54
2.1 Before initiating MLA: Intelligence gathering and informal methods of cooperation	55
2.2 When to request MLA: Timing of the request	55
2.3 How to request MLA: Legal basis	56
2.4 What to request through MLA: Types of assistance	57
2.5 How to request MLA: Dual criminality	57
2.6 How to request MLA: Speciality	58
3. Step 2: Drafting MLA	58
3.1 Final consideration: Fishing expedition	59
3.2 Language of the request	59
4. Step 3: Submitting a request for MLA	59
Annex 1 - MLA checklist	61
Annex 2 - Model request for MLA	63



## 1. Introduction

Identifying the proceeds of crime is often a complex and time-consuming process that frequently crosses national borders, as evidence and assets are not always found exclusively in the state conducting the investigation, prosecution or judicial proceedings. As a result, one state will normally require the assistance of other states in locating offenders, witnesses, evidence and, in particular, assets. Stolen assets are usually quickly removed abroad to try to get them out of reach of the investigating jurisdiction where the predicate offence takes place – hence the particular importance of international cooperation in identifying, locating and seizing stolen assets.

States have developed processes for requesting and obtaining information, evidence and the seizure of assets for cross-border investigations and prosecutions. They normally start through a mutual exchange of information, police-to-police or via FIUs (Financial Intelligence Units) (see chapter 5), followed by what is known as a request for mutual legal assistance. The informal mutual sharing of information should be used first to help inform and direct the subsequent request for MLA. A request for MLA is sent by one state (the requesting state) to another state (the requested state), which may in turn trigger an incoming request for MLA to the requesting state from the requested state. There are certain legal and practical requirements this chapter discusses.

MLA is important to a number of procedures that comprise the asset recovery process: it is conducted during the investigation, prosecution or trial phases of the criminal proceedings to identify and restrain assets linked to the proceeds of crime with a view to their ultimate confiscation and repatriation post conviction. The main difference between the formal and informal ways of gathering information lies in the fact that the formal MLA route generally allows a requested country's response, statements and supporting documents to be used as admissible evidence in the requesting country's jurisdiction, and *vice versa*.

One of the main problems facing a requesting country with

stolen assets that are based outside its jurisdiction is linking those assets to a crime that occurred within its jurisdiction. Establishing that a predicate offence has occurred is not enough; there also needs to be a link between the predicate offence to the assets held abroad. At this initial stage, such a link need not have to be established via evidence for the purpose of a request for MLA. An investigation theory or suspicion or belief from a requesting state linking the assets to an offence usually will be sufficient for the requested state to respond.

Finally, consideration should be given to the fact that requests for MLA are time-sensitive, and their effectiveness (in particular, when dealing with the need to act quickly to freeze stolen assets) to a very large degree depends upon the trust and cooperation established through the informal sharing of information.

### *Scope and purpose*

Through MLA, the requesting state seeks the requested state, among others: (i) to satisfy evidentiary requirements with regard to the investigations, prosecutions or court proceedings being conducted in the requesting state; or (ii) to safeguard assets which are believed to be the proceeds of crime and are found in the requested state and may be at risk of dissipation. The aim of requesting MLA is to ultimately enforce in the requested state a final confiscation order from the requesting state with a view to repatriating the confiscated assets. Thus, requests for MLA will be needed to produce evidence or to safeguard assets (these can be done jointly or in separate requests for MLA, depending on the case strategy) and to recognise and to enforce the final confiscation order.

MLA may be sought by the requesting state at any stage of the proceedings – be they investigation, prosecution or court proceedings. MLA is based on mutual coordination, cooperation and communication. Therefore, requests must contain sufficient information – obtained through an investigation in the requesting state – for the requested state to understand the facts and the context of what is being sought and to connect them with the assets whose

seizure is being requested, thereby enabling the requested state to act on behalf of the requesting state.

MLA allows evidence to be secured or assets found in a foreign jurisdiction to be traced, identified, preserved, constituted, secured, confiscated or returned in a legally valid manner for the requesting state. The actions undertaken on behalf of the requesting state by the requested state through MLA are legal, and their results in the requested state are to be used exclusively in the proceedings of the requesting state specified in the request for MLA.

MLA is necessary because the requesting state cannot exercise its authority directly in the requested state, and thus the latter requires prior authorisation from the former to do so. When issuing a request for MLA, the requesting state must therefore also observe the legal and constitutional requirements of the requested state. Thus, MLA becomes the process through which a request is submitted and the manner in which the requested state becomes empowered to furnish evidence or take coercive measures on behalf of the requesting state. This way, MLA complies both with the legal requirements of the requested state and ascertains the actions carried out through it are valid in the courts of the requesting state.

## 2. Step 1: Preparing for MLA

Prior to drafting a request for MLA, the requesting authority must determine the following:

- Whether to use the MLA channels or another intelligence or informal method of cooperation;
- Timing for submitting the request for MLA;
- Status of the authority requesting MLA;
- Type of assistance sought;
- Legal basis for the request; and

- Criminal offence(s) under investigation.

The authority responsible for issuing the request for MLA (requesting authority) must know and understand the international requirements and those of the requested state needed for a successful request. It must also establish the object of the assistance sought from the requested state. Furthermore, the requesting authority must know when the request for MLA must be accompanied by additional supporting documents, such as a court order for the preservation of assets to be enforced in the requested state.

All these elements need to be known by the requesting authority before the actual request is submitted to the requested state. In order to identify them, the requesting authority must make prior contact with the requested state. This contact should be informal where possible and feasible (e.g. via an email or phone call), and the requesting authority should either contact a counterpart in the requested state, where known, or request guidance on the matter from the central authority of the requesting state. The requesting authority should describe the following in its request for clarification:

- The criminal offence(s) under investigation in the requesting state;
- The information, evidence or assistance being sought in the requested state; and
- The legal, evidentiary and other specific requirements for obtaining assistance from the requested state.

Therefore, prior to submitting any request for MLA, the requesting state must first put in place a case strategy (as described in chapter 2) relating to the investigation or prosecution of the matter, making sure that any MLA requirements are absorbed into such case strategy. The requesting state, while responsible for the investigation and prosecution, must thoroughly analyse all facts and elements surrounding the investigation or prosecution, and determine (i) what actions need to be taken; (ii) when each action should

be initiated; and (iii) what to anticipate, understand and acknowledge regarding the implied risks and consequences of each of the actions taken.

### **2.1 Before initiating MLA: Intelligence gathering and informal methods of cooperation**

The requesting authority must determine whether requesting MLA is the most appropriate course of action for the purposes intended in their investigation or prosecution. The requesting authority must first determine whether the information sought is to be used for intelligence or for evidentiary purposes. Should the former be the case – that is, if no evidence is to be presented to a court or coercive measures sought but rather the collection of information in support of an investigation or prosecution – the requesting authority may collect such information through intelligence gathering mechanisms or informal assistance.

Determining the end use of the information sought enables the requesting authority to better determine the level of formality needed to obtain the information and, consequently, the speed with which the information can be obtained. This is because informal assistance does not require the same level of formalities as MLA. However, obtaining information through informal means does not, generally, constitute evidence due to the fact that it lacks the necessary formalities agreed upon between requesting and requested states. Nevertheless, it enables the investigator or prosecutor to draw leads for the investigation or prosecution in a swifter fashion, which may lead to a request for MLA to gather the necessary evidence or apply provisional measures.

While it is not possible to prescribe the scope of application of informal methods of cooperation, they generally include non-coercive investigative measures, such as gathering publicly available information, conducting visual surveillance and obtaining information from Financial Intelligence Units (FIUs). They may additionally extend to spontaneous disclosures of information (Article 46(4) UNCAC).

As opposed to MLA, which has clearly defined channels of transmission (see section 4. below), informal assistance is carried out between counterparts directly (through a telephone conversation or face-to-face meetings) or through one of several informal networks created for such purposes.<sup>1</sup> Additionally, there are several formalised networks that enable the sharing of financial or police intelligence between authorities. These are the Egmont Group and Interpol.

### **2.2 When to request MLA: Timing of the request**

The timing for submitting a request for MLA is also important. Communication is paramount so that both the requested and the requesting states fully understand the outcomes, results and consequences of any assistance rendered. As stated above, there is an overriding need to establish a link between the crime alleged to the assets held in the requested state. It is only through appropriate communication that the practitioner will learn and understand the legal implications of the request in the requested state. Moreover, understanding these implications will also anticipate legal challenges in the proceedings in the requesting state.

Other factors affecting the timing of the request include issues of urgency and confidentiality related to the request for MLA. The requesting state must communicate any reasons for urgency to the requested state, so that it may render the assistance within the given timeframe (or anticipate that it is not possible to do so). Issues of confidentiality should be mutually discussed before sending a request, because a requested state may be obligated to disclose evidence to the defence prior to sending it to the requesting state. Also, prior to drafting a request for MLA, it is important to identify the competent authority responsible for issuing the request (requesting authority). International treaties are normally silent in this regard, as it is understood that this

<sup>1</sup> These are, among others: the Camden Assets Recovery Inter-Agency Network (CARIN); the Red Iberoamericana de Cooperación Jurídica Internacional (IBERRRED); the Red de Recuperación de Activos de GAFILAT (RRAG); the Asset Recovery Inter-Agency Network of Southern Africa (ARINSA).

is a matter to be determined by the procedural laws of the requesting state.

As a general rule, however, the requesting authority will be the lead authority (referred to as the competent authority) responsible for the phase of the criminal proceedings during which the request for assistance arises. Therefore, if the request is issued during the investigation phase, the person responsible for the investigation should file the request for MLA. Conversely, if the investigation has been finalised and the criminal proceedings are in the prosecution phase, the prosecutor should file the request for MLA. Finally, if the criminal proceedings are at the trial phase, the court should file the request for MLA. Identifying the correct requesting authority is crucial, given that any assistance provided in response to the request for MLA may be invalid in the proceedings of the requesting state if it has not been requested by the correct authority empowered to do so.

Moreover, it should be noted that there are exceptions to the general rule stated above. These exceptions frequently derive from the laws of the requested state. One example relates to a request for MLA during the investigation phase: in many jurisdictions, investigations are carried out by law enforcement agencies (LEAs), which are completely independent from the prosecution. In others, however, the prosecutor’s office is responsible for the investigation, which then delegates its powers to law enforcement. Thus, some jurisdictions that do not have an independent LEA may not accept a request stemming from a LEA and require that a prosecutor of the requesting state issue the request instead.

### 2.3 How to request MLA: Legal basis

In determining the legal basis for the request for MLA, the requesting authority must take the following into consideration: (i) bilateral or multilateral international

treaties;<sup>2</sup> (ii) reciprocity undertaking; or (iii) the use of enabling legislation of the requested state. These options are not self-excluding and are complementary to each other.

A multilateral or bilateral treaty may be invoked for the purpose of MLA if both the requesting and requested states have ratified it. Treaties in force between the requesting and requested jurisdictions create an international obligation to cooperate between the jurisdictions involved in the matters specified in the treaty that is being invoked.

In the absence of an enabling treaty, the requesting state may request MLA (or the requested state may render it) through a reciprocity undertaking: the requesting state undertakes to provide reciprocal treatment to the requested state in future cases of a similar nature to that of the object of the request.

Finally, the requesting state may also request assistance on the basis of any enabling internal legislation on MLA in existence in the requested state.<sup>3</sup> Several jurisdictions already have within their legal framework provisions for the receipt, processing and execution of foreign requests

2 These are, among others: the **United Nations Convention Against Transnational Organised Crime (UNTOC)**, available at [https://www.unodc.org/documents/middleeastandnorthafrica//organised-crime/UNITED\\_NATIONS\\_CONVENTION\\_AGAINST\\_TRANSNATIONAL\\_ORGANIZED\\_CRIME\\_AND\\_THE\\_PROTOCOLS\\_THERETO.pdf](https://www.unodc.org/documents/middleeastandnorthafrica//organised-crime/UNITED_NATIONS_CONVENTION_AGAINST_TRANSNATIONAL_ORGANIZED_CRIME_AND_THE_PROTOCOLS_THERETO.pdf); the **United Nations Convention Against Corruption (UNCAC)**, available at [http://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026\\_E.pdf](http://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf); the **Inter-American Convention on Mutual Legal Assistance in Criminal Matters**, available at <http://www.oas.org/juridico/english/treaties/a-55.html>; and the **Convention on Legal Assistance and Conflicts of Law in Matters of Civil, Family and Criminal Law**, available at [http://www.hcch.net/upload/wop/jdgm\\_info01e.pdf](http://www.hcch.net/upload/wop/jdgm_info01e.pdf).

3 Several states have developed guidelines with a view to assisting requesting states in understanding their legal systems and the requirements that need to be met for issuing requests for MLA. These can be found at, among others: <https://star.worldbank.org/star/ArabForum/asset-recovery-guides> (for many European states, the US, Canada, Japan and Hong Kong) or <http://www.oas.org/Juridico/mla/en/index.html> (for members of the Organisation of American States).



for MLA, e.g. Switzerland and the United Kingdom.<sup>4</sup> These laws provide the conditions, rules, duties and limitations of a request for MLA emanating from a foreign jurisdiction.

## 2.4 What to request through MLA: Types of assistance

Treaties on MLA generally provide for types of assistance which may be sought. The types of assistance are, however, not exhaustive and states will render assistance insofar as the request does not contradict its own internal constitutional and legal framework. However, it should be noted that a request may be postponed, conditioned, partly executed or altogether refused – even when all the conditions have been met – when executing the request for MLA may interfere with an ongoing investigation, prosecution or judicial proceeding.

The list below contains the generally accepted activities that can be undertaken through MLA and found in international treaties dealing with MLA (such as the United Nations Convention Against Transnational Organised Crime [UNTOC] and the United Nations Convention Against Corruption [UNCAC]). It should be underscored that the requesting and requested states may render any other type of assistance that is not on the list below and that is not contrary to the domestic law and fundamental principles of the requested state.

Therefore, MLA can be rendered, among others, for the following purposes:

- Taking evidence or statements from persons;
- Effecting service of judicial documents;
- Executing searches and seizures, and freezing;

- Examining objects and sites;
- Providing information, evidentiary items and expert evaluations;
- Identifying, freezing and tracing proceeds of crime;
- Providing originals or certified copies of relevant documents and records, including government, bank, financial, corporate or business records;
- Identifying or tracing proceeds of crime, property, instrumentalities or other items for evidentiary purposes; and
- Facilitating the voluntary appearance of persons in the requesting state.

## 2.5 How to request MLA: Dual criminality

The principle of dual criminality (provided for in Article 43(2) and 46(9)(b) UNCAC; Article 18(9) UNTOC) provides that the criminal offence under investigation in the requesting state must correlate to one in the requested state. The offence in both the requesting and requested states does not have to be identical – were this to be required, it would greatly diminish the possibility of rendering assistance or coordinating different legal systems and traditions. Dual criminality means that the core elements, or substance, of the offence in both states must be similar in nature.

Prior to drafting the request for MLA, the requesting authority must be aware of any dual criminality considerations. Thus, it must communicate with the requested state, explaining the elements of the criminal offence and how these are required in order to prove the criminal offence under investigation or prosecution. Communication is key: the requesting authority must rely heavily on communication with the requested state in order for the issue of dual criminality to be properly understood.

<sup>4</sup> For Switzerland, this is the Federal Act on International Assistance in Criminal Matters, available at <http://www.admin.ch/opc/en/classified-compilation/19810037/index.html>. For the United Kingdom, this is the Crime (International Co-operation) Act 2003, available at [http://www.legislation.gov.uk/ukpga/2003/32/pdfs/ukpga\\_20030032\\_en.pdf](http://www.legislation.gov.uk/ukpga/2003/32/pdfs/ukpga_20030032_en.pdf).

## 2.6 How to request MLA: Speciality

The principle of speciality prohibits or prevents the requesting state from utilising the results arising from the assistance rendered by the requested state in proceedings other than those specified in the request for MLA. This does not mean, however, that the results from such a request cannot be utilised in proceedings other than those specified in the request for MLA. Rather, it means that the requesting state must ask in writing for permission from the requested state to utilise the results in other proceedings and obtain such authorisation prior to disclosing the evidence in other proceedings. This written request must refer to the new proceedings in which the requesting state wishes to use the evidence, explaining the offences under investigation, the context of the investigation and how the evidence provided would benefit the other proceedings. Should the requested state agree, the evidence may then be lodged in the new proceedings, respecting any conditions that the requested state may wish to impose.

## 3. Step 2: Drafting MLA

Once it is determined that a request for MLA is necessary, the first step to be taken prior to drafting the request is **communication**. This entails calling or sending an e-mail to one's counterpart in the requested state or making contact with the central authority of one's country. The requesting authority should communicate with the requested state to understand what its requirements entail. Preparing a request for MLA must be thorough and complete, as the main goal is to guarantee its effectiveness and the desired results.

The request for MLA must contain **basic identification information**, which includes:

- Full name of the person(s) under investigation or prosecution (as well as his or her known aliases), date of birth, names of the parents of the person under investigation or prosecution, his or her nationality(ies) and the number of his passport(s) with date of expiry

and issuing country; and

- Identification of the proceedings giving rise to the request of MLA, including the investigation docket number, nature of the proceedings and stage of the criminal proceedings in respect of which the request for MLA being made.

Following the basic information, the requesting authority enters the **narrative section of the request** for MLA, which contains the following:

- **Facts of the case.** The narrative of the request for MLA must at all times remain straightforward, simple and objective, as the requested state must understand the correlation between the criminal activity in the requesting state, the person(s) who have allegedly committed the offence, the unlawful assets which resulted from, or which were instruments of, the criminal activity and what is being requested. The assistance sought should be clearly established and linked to the facts and criminal conduct described in the request. Simple, clear and objective are keywords – the requesting authority should take into consideration that the recipient authority is not an expert in the laws of the requesting state and must understand their laws and concepts, particularly in order to determine issues of dual criminality described above.
- **Description of the assistance sought.** The requesting authority will need to detail to the requested state what actions are required in respect of the proceedings underway in the requesting state. The requesting authority should try to provide as much information as possible to facilitate the activities needed to be undertaken through the request for MLA. This section should be well coordinated with the requesting state prior to the formal submission of the request to ensure its full compliance with the laws of the requested state.

- **Objectives of the request.** The requesting authority needs to explain to the requested state for which purpose the above-mentioned actions are sought through the request and the expected outcomes.
- **Any procedures to be observed.** Requests for MLA are executed in accordance with the laws of the requested state. Nevertheless, the requesting state may require that special procedures be observed during the execution of the request (e.g. urgency in the execution of the request, secrecy in the execution of the request, particular procedures that should be followed in the requested state while executing the request). In so doing, the requested state must comply with these special procedures, insofar as they are not incompatible with the laws and regulations of the requested state.
- **Transcription of the criminal offences.** All criminal offences under investigation should be fully transcribed in the request for MLA, be it in the body of the text or as an annex to the request. The transcription of the criminal offence is important so that the requested state understands the legal definition of the criminal offence (for dual criminality purposes) and is aware of the punishment that is provided in respect of the criminal offence in question.

### 3.1 Final consideration: Fishing expedition

Despite this broad application of MLA, it should not be mistaken for a transfer of the responsibility to investigate to the requested state (commonly known as a fishing expedition). MLA is not a request for the requested state to conduct an investigation or prosecution for or on behalf of the requesting state. Instead, the requesting state must conduct its own investigation and request assistance for the production of evidence that the requested state possesses. This evidence will corroborate and clarify certain facts or leads for the requesting state. The requesting state's preliminary investigations must have shown evidence that this is the case and must have provided details about the

assets to be found in the requested state (e.g. the bank in which the account is held).

### 3.2 Language of the request

Requests for MLA are written in the official language(s) of the requesting state. However, the official language of the requested state may not be the same as the language of the requesting state. As a result, the requesting state must submit the request for MLA translated into the official language (or one of the official languages) of the requested state. The responsibility for the translation of the request lies with the requesting state.

Given that a request for MLA may need to be translated, the requesting authority should always strive to use simple, short and straightforward sentences to avoid any misinterpretation of any aspect of the request. If the requested authority is unable to understand the request for MLA, it will not be able to process and execute the request.

In exceptional and urgent circumstances, however, the requesting and requested states may mutually agree to submit and receive a request for MLA in a common designated language (e.g. English) for faster processing of the request. In such circumstances, the requesting state will still have the obligation to submit the request ultimately in the official language (or one of the official languages) of the requested state.

## 4. Step 3: Submitting a request for MLA

Once the requesting authority determines that a request for MLA should be issued, it must determine the form of transmission of the request.

- Transmission via diplomatic channels is the general rule. In the absence of any enabling treaty ratified by the requesting and requested states, the former must transmit its request for MLA via diplomatic channels.

- Transmission via central authorities is possible when an enabling agreement between the requesting and requested states allows for the transmission of requests in this manner. Central authorities are specialised bodies in MLA.<sup>5</sup> They are set up by states to guide their national authorities, as well as states requesting MLA, with regard to the requirements needed to submit a request for MLA.
- Direct transmission of requests for MLA is only possible through certain regional treaties where the requesting authority is authorised to submit requests for MLA directly to the executing authority in the requested state without the need for transmission via central authorities or diplomatic channels.

The requesting authority should be aware that whatever the mode of transmission, it will entail a relatively long delay from the transmission of the request to its receipt and actual execution by the requested state. Given this delay, and only in urgent circumstances, a draft of the request for MLA should be forwarded to the requested state through mutually agreed means of communication (e.g. fax, email, etc.) with the original following through formally identified channels. Also, prior to advancing a draft, the requesting authority should communicate this fact to the requested state.

---

<sup>5</sup> A central authority (Art. 46(13) UNCAC; Art. 18(13) UNTOC) is a body (or, less frequently, bodies) that is responsible for providing assistance to the requesting state or in seeking assistance from the requested state. Central authorities are tasked with either arranging for the receipt and execution of requests for MLA, or facilitating the execution of such requests. Depending on the country, the central authority may be located in the Ministry of Justice, Ministry of Foreign Affairs or at the Prosecution Service.

# Annex 1 - MLA checklist

Preparation for Mutual Legal Assistance	Has the competent requesting authority been established?
	Has there been mutual sharing of relevant intelligence?
	Has a first contact regarding your case been established with the requested state?
	Have you established what are the criminal offences under investigation?
	Have you (or your central authority) verified whether the criminal offences under investigation meet the dual criminality requirement in the requested state?
	Have you established the assistance required from the requested state?
	Is the assistance required available publicly? <i>If so, consider using intelligence channels or informal channels of communication.</i>
	Must the information required be obtained formally or informally? <i>If information can be obtained informally, consider using intelligence channels or informal channels of communication.</i>
Drafting Mutual Legal Assistance Requests	Have you (or your central authority) established the legal basis for the request for MLA?
	Have you fully and properly identified the person under investigation?
	Have you indicated all the proceedings relevant to the request for MLA as well as their current status?
	Have you identified all the criminal offences for the purpose of checking with the requested state that dual criminality requirements have been fulfilled?
	Have you indicated all the applicable criminal offences in the request for MLA?
	Have you included a transcription of all the relevant criminal offences in the request for MLA?
	Have you determined the object of the request for MLA?
	Have you (or your central authority) discussed the object of the request for MLA with the requested state and verified it with regard to relevant thresholds? <i>Verify what are the evidentiary standards in the requested state for the criminal offences indicated. Also ensure with the requested state that the narrative in the request for MLA fulfils all the elements of the offence in accordance with the laws of the requested state.</i>
	Have you presented in your request for MLA all the relevant facts for the requested state?
	Have you through a clear, direct and straightforward narrative indicated the connection between the persons under investigation and the relevant facts presented?
	Have you through a clear, direct and straightforward narrative indicated the connection between the relevant facts and the criminal offences?
	Have you through a clear, direct and straightforward narrative indicated the connection between the facts and the object of the request for MLA? <i>The object of the request must be contextualised in the request for MLA. It can range from within the purposes indicated in section 2.5. For example, if the object of the request is the seizure of a bank account, the request should, through its narrative, indicate how the specific bank account connects to the facts of the case as well as the person(s) who have allegedly committed the criminal offence.</i>

	Have you clarified for the requested state the relevance of the object of the request for MLA?
<b>Submitting Mutual Legal Assistance Requests</b>	Have you verified the legal basis for the request for MLA?
	Have you established the mode of transmission of the request for MLA?
	If applicable, have you (or your central authority) translated the request for MLA into the official language of the requested state?
	If the request is to be kept confidential, have you expressly indicated this in the request for MLA, explained and given the reasons for such confidentiality?
	If urgent, have you (or your central authority) made previous contact with the requested state in the matter prior to submitting the request for MLA?
	If urgent and agreed upon, have you (or your central authority) submitted an advance copy of the request for MLA?

# Annex 2 - Model request for MLA

<b>Legal basis for the request:</b>	Indicate here all the legal bases on which the request is being formulated, e.g. UNCAC, a bilateral treaty, the internal legislation of the requested jurisdiction, reciprocity undertaking.  <i>e.g. This request is made pursuant to the United Nations Convention Against Corruption, ratified in (indicate name of the requesting state) through Law/Decree/By-law No.</i>
<b>Requesting authority:</b>	Indicate the identity of the requesting authority. The requesting authority should include here its name and contact information – email and telephone number. Provide also details indicating the role and functions of the requesting authority so that the requested state is satisfied it has the competence to deal with requests for MLA. It must be established that the requesting authority in the requesting state has the authority to either investigate or prosecute, or both, in terms of its domestic legislation.
<b>Recipient (requested) authority:</b>	Indicate the central authority of the requested jurisdiction. If previous contact with a specific authority has been made, consider also including the name and contact information of this authority.  <i>e.g. Federal Office of Justice of Switzerland – Central Authority for Mutual Legal Assistance</i>
<b>(Case) Reference:</b>	Indicate the (case) reference of the requesting authority, e.g. the case file number or name of the operation/main perpetrator.  <i>e.g. Request for Mutual Legal Assistance in the matter of XYZ</i>
<b>Proceedings:</b>	Indicate a brief summary of the request for MLA. The summary should provide a brief snapshot that will enable the reader to quickly identify the request and establish priorities. This summary should include the following:  Indicate (i) the docket number; (ii) the stage of the proceedings reached in the case (investigation, prosecution or trial); (iii) the identity of the individual against whom proceedings are pending or instituted; and (iv) for which alleged criminal offences.  <i>e.g. Criminal Investigation No. 123, before the (indicate authority), against (indicate name of investigated person(s)), for possible criminal activity related to (indicate criminal offences).</i>
<b>Criminal offences:</b>	Include all the criminal offences which are under investigation or prosecution and that directly relate to the request for MLA. The full text of the criminal offence should be placed at the end of the request for MLA or as an annex to it.

<b>Persons under investigation:</b>	Include (i) the full name and aliases of the person(s) under investigation or prosecution as well as all forms of international identification; (ii) date of birth (DOB); (iii) name of parents; (iv) passport number(s) with date of expiry; and (v) any known address(es).
<b>Facts:</b>	<p>This is the most important section of the request for MLA. The relevant facts of the case, which are also connected to the requested state should be presented in the request for MLA.</p> <p>The facts should include the relation of the person(s) under investigation, prosecution or trial to the facts of the case and evidence presented, the criminal offence for which the person(s) was charged, the assets that have been identified during the investigation or prosecution, the connection of these assets with the facts of the case as well as the assistance being sought in the request for MLA.</p> <p>The facts should be presented in short, direct, clear and straightforward sentences. Remember: the requested state may not speak your national language (requiring the translation of the request) and is not an expert in your national law.</p> <p><i>e.g. On XXXX (date), the XXXX (details of the authority which instituted the criminal investigation) instituted an investigation into the affairs of Company X with specific reference to the activities of, inter alia, individuals A and B. It is apparent that a prima facie case involving the following offences, namely:</i></p> <ol style="list-style-type: none"> <li>1. XXXX</li> <li>2. XXXX</li> </ol> <p><i>has been established against officials and/or shareholders of this company, to wit:</i></p> <ol style="list-style-type: none"> <li>1. XXXX</li> <li>2. XXXX</li> </ol>
<b>Transcription of the criminal offences:</b>	Transcribe any and all articles of law mentioned in the 'criminal offences' and 'facts' sections above. For criminal offences, these should include the title of the criminal offence, the description of the criminal offence and the relevant penalty. The transcription of the criminal offences may also be placed as an annex to the request for MLA.
<b>Description of the assistance sought:</b>	State what is needed from the requested authority and how you would like it to be done. Try to give as much detail as possible. This section should be well coordinated with the requesting state prior to the request being submitted.



<b>Objectives of the request:</b>	State how the assistance rendered will assist the investigation or prosecution in the requesting state.
<b>Procedures to be observed:</b>	<p>State if there are any procedures to be observed, such as confidentiality or urgency.</p> <p><i>e.g. <b>Reciprocity:</b> The government of the XXX (requesting state) confirms that if the government of the XXXX (requested state) complies with this request, the XXXX (requesting state) will comply with future requests from the government of the XXXX (requested state) for legal assistance in criminal matters.</i></p> <p><b>Speciality:</b> The government of the XXXX (requesting state) provides the undertaking that any evidence and/or information provided by the government of the XXXX (requested state) and transmitted to the XXXX (requesting state) will not be used for the investigation and prosecution of any crimes other than those stated in this request without the prior permission of the XXXX (requested state).</p> <p><b>Confidentiality:</b> If the details of the request are to be kept confidential, this must be stated in the request, e.g. if it is feared that the suspect will destroy evidence or dissipate assets, then this must be brought to the attention of the requested state.</p>
<p><b>Signature of requesting authority</b></p> <p><b>Place and date</b></p>	



# 5. Using the anti-money laundering framework in asset tracing

Elena Hounta | Selvan Lehmann

- 1. Introduction **69**
- 2. The anti-money laundering (AML) framework **70**
- 3. The use of AML suppressive measures in asset tracing **72**
  - 3.1 Provisional measures **72**
  - 3.2 Provisional measures for cases with an international dimension **72**
  - 3.3 Confiscation and the reversal of the burden of proof **73**
  - 3.4 Non-conviction based confiscation **74**
  - 3.5 Range of assets subject to freezing, seizing and confiscation **75**
- 4. The use of AML preventive measures in asset tracing **75**
  - 4.1 Requirements in customer due diligence (CDD) and record keeping **76**
  - 4.2 Identification of politically exposed persons (PEPs) **78**
  - 4.3 Targeted financial sanctions related to individuals and entities **79**
- 5. The role of the Financial Intelligence Units (FIUs) in asset tracing **80**
  - 5.1 Types of FIUs **80**
  - 5.2 Reporting obligations and information received by FIUs **82**
  - 5.3 The role of FIU in financial investigations and adding value to data **84**
  - 5.4 Dissemination of information to other authorities **87**
- 6. The role of national and international cooperation in asset tracing **88**
  - 6.1 Cooperation at national level **88**
  - 6.2 Cooperation at international level **89**



## 1. Introduction

Members of organised crime or individuals who are engaged in criminal activities with a financial dimension have as goals: to hide the proceeds obtained from such illegal activities, and if these proceeds have been traced by law enforcement agencies (LEAs), to ensure that they cannot be linked to the illegal activities. Money laundering is a mechanism that relates exactly to these goals and is generally understood as the process through which the illegally obtained proceeds of a criminal activity are converted/transformed into ostensibly legitimate money or other assets in order to conceal/disguise their illicit origin or source. It is a crime that always requires the commission (but not conviction) of another crime, a predicate offence, such as drug trafficking, corruption, fraud, embezzlement, activities of criminal organisations, tax evasion, terrorist financing.

The international community has recognised the seriousness of the money laundering offence and its implications for the financial system. The offence has been criminalised and specifically defined in international conventions, including the 1988 United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention), the 2000 United Nations Convention Against Transnational Organised Crime (Palermo Convention) and the 2004 United Nations Convention Against Corruption (UNCAC).<sup>1</sup>

<sup>1</sup> According to Article 6 of the Palermo Convention, money laundering refers to: (a) (i) the conversion or transfer of property, knowing that such property is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of the property or of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of his or her action; (ii) the concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime; and (b) (i) the acquisition, possession or use of property, knowing, at the time of receipt, that such property is the proceeds of crime; (ii) participation in, association with or conspiracy to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the offences established in accordance with this article.

### DEFINITION - MONEY LAUNDERING

Money laundering is a process by which illegally obtained proceeds of a criminal activity are converted/transformed into ostensibly legitimate money or other assets in order to conceal/disguise their illicit origin or source.

### DEFINITION - FINANCIAL ACTION TASK FORCE (FATF)

Financial Action Task Force (FATF) is an inter-governmental body which sets the standards for the measures that countries need to take to combat money laundering as well as terrorist financing, and issues respective recommendations in order to strengthen the financial system against financial crime.

Furthermore, in 1989 the G-7 Summit established an inter-governmental body under the name 'Financial Action Task Force' (FATF) in response to the fight against money laundering. Since then the FATF remains the main player and standard-setter in the fight to combat money laundering and terrorist financing. It has also issued respective recommendations in order to strengthen the financial system against financial crime.

The international anti-money laundering (AML) framework can be used by practitioners as a tool in the process of tracing illegal assets, depending, of course, on the degree of its implementation in the relevant country's legal system. This chapter will briefly describe the AML framework and then seek to identify the role and use of the various aspects thereof in tracing illegally obtained assets. The chapter will be divided into the following subchapters:

1. The AML framework;
2. The use of AML suppressive measures in asset tracing;
3. The use of AML preventive measures in asset tracing;

4. The role of Financial Intelligence Units (FIUs) in asset tracing; and
5. The role of national and international cooperation in asset tracing.

## 2. The AML framework

The AML framework is based mainly on international conventions as well as the recommendations and guidance issued by the FATF. The FATF had originally issued 40 Recommendations relating to money laundering and 9 relating to terrorist financing. In 2012, however, the Recommendations were revised and redrafted to form a total of 40 Recommendations.<sup>2</sup>

Some of the main results of the last revision of the Recommendations can be summarised as follows:<sup>3</sup>

- **Broader range of standards.** The standards address new threats, such as proliferation of weapons of mass destruction, corruption and tax crimes, while the requirements for identifying politically exposed persons (PEPs) as well as for providing transparency regarding legal persons and arrangements have been strengthened.
- **Centralisation of the risk-based approach (RBA).** The RBA is used when a country conducts a national risk assessment (NRA) with the aim to identify and assess the risks that money laundering and terrorist financing impose on the market, the people involved and the products. The NRA serves as a

basis to adjust the national anti-money laundering/ countering financing of terrorism (AML/CFT) system by focusing on those risks identified in the NRA. Enhanced measures should be taken when the risks are higher and simplified measures should be taken when the risks are lower so that better allocation of the country’s available resources is achieved.

- **Adoption of a new assessment methodology by FATF.** The FATF evaluates countries’ compliance with the Recommendations based not only on technical assessment but most importantly on effectiveness assessment and to what extent the countries achieve a defined set of outcomes central to a robust AML/CFT system.

The AML framework can be described as follows (see figure 1 below):<sup>4</sup>

At the core of the framework, one finds the criminal offences (money laundering and/or terrorist financing) for which suppressive as well as preventive measures need to be established, such as those listed in Figure 1 below. For such measures to be effective there should be regulation and supervision, empowerment of LEAs and FIUs, as well as international cooperation. The overarching principle is the RBA, which should be used to evaluate and provide focus for the framework at national level and also be reflected in the NRAs conducted by the countries.

2 FATF, ‘International Standards on Combatting Money Laundering and the Financing of Terrorism and Proliferation, The FATF Recommendations’. Available at [http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF\\_Recommendations.pdf](http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf), viewed on 21 November 2014.

3 FATF, ‘FATF Recommendations, Media Narrative’. Available at <http://www.fatf-gafi.org/media/fatf/documents/Press%20handout%20FATF%20Recommendations%202012.pdf>, viewed on 21 November 2014.

4 The FATF Recommendations, op. cit.

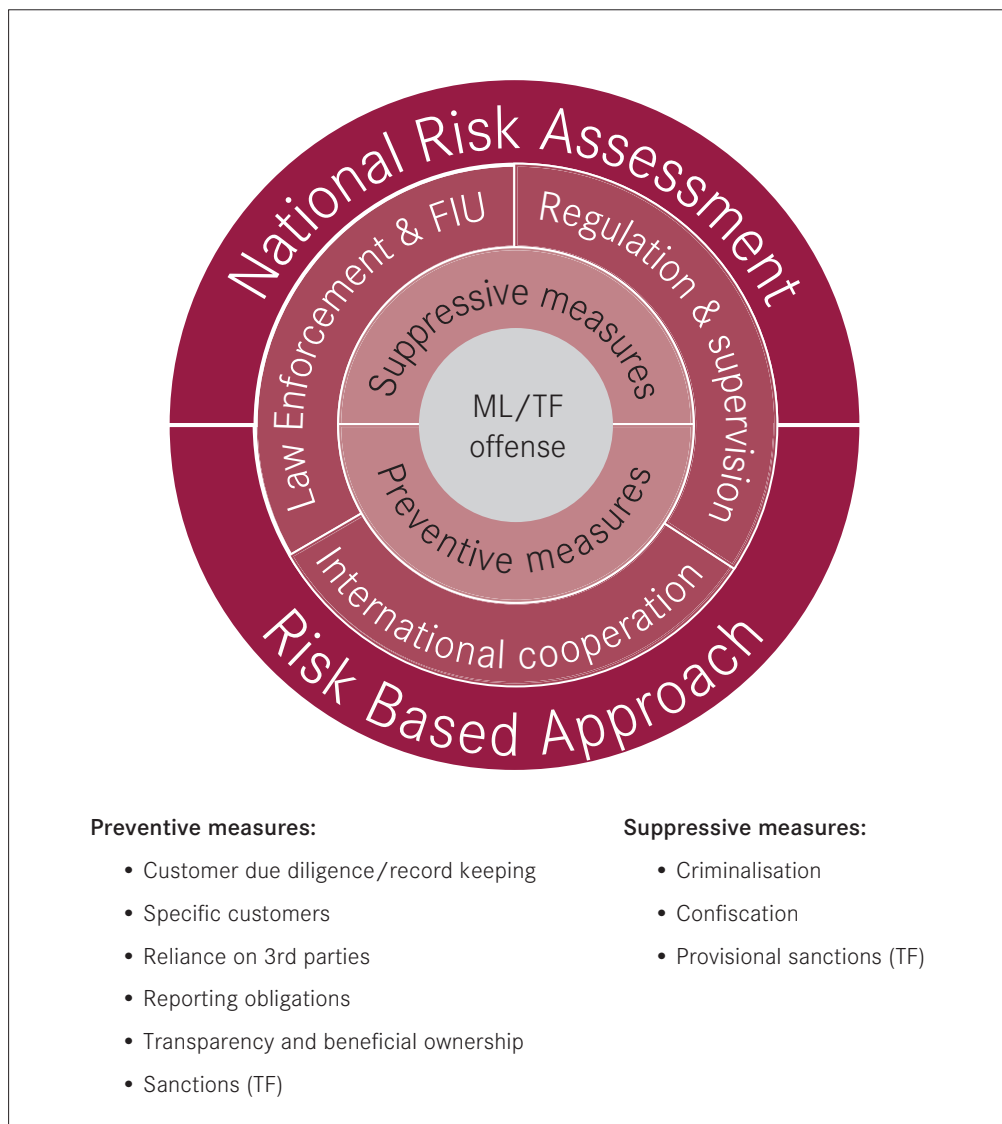


Figure 1 - AML/CFT Framework

### 3. The use of AML suppressive measures in asset tracing

The AML framework requires countries to adopt suppressive measures, such as criminalising the offence of money laundering, adopting provisional measures and establishing effective confiscation procedures. Provisional measures include freezing and seizing of assets, whereas confiscation is a final measure ordered at the very end of the criminal process. The national competent authorities should be able to freeze, seize and confiscate illegally obtained assets.

Practitioners should be aware of the following aspects of the AML framework relating to provisional measures and confiscation when tracing illegally obtained assets.

#### 3.1 Provisional measures

Provisional measures aim to secure and prevent the disappearance of illegally obtained assets and mainly relate to the freezing or seizing of assets. Those measures should be in place while handling domestic cases as well as while facilitating relevant requests by foreign jurisdictions.

Freezing is a provisional measure applicable to bank accounts and other financial products that prevents the nominative owner of such products from moving, transferring or converting these assets. Freezing is a measure that must be approached carefully to ensure that it is taken at the appropriate moment during the process. Once assets are frozen, the investigator or prosecutor runs the risk of alerting the target to the investigation, which could hinder the tracing of other assets. Furthermore, following the movement of assets could lead the investigator to other accounts where further funds may be stashed, even proceeds from different offences. If assets are frozen prematurely, the investigator may lose the opportunity to find other accounts. On the other hand, if assets are frozen too late, the trail may be lost. Whilst criminals can move their funds around very quickly and conceal them very effectively, law enforcement takes much longer to trace them, as investigators are bound by

the law. Consequently, investigators must take into careful consideration the most appropriate time to freeze assets.

Seizing is a provisional measure applicable to movable or immovable property that prevents the nominative owner of such property from selling or transferring it, ideally for the duration of the criminal process. Certain issues must be taken into account when dealing with the seizure of assets, particularly the nature of the assets to be seized. Assets that depreciate easily and require high maintenance costs, high-risk or perishable assets, livestock and precious woods must be carefully assessed before seizure, as alternatives to seizing might be more appropriate.

Practitioners should be aware that for AML purposes the above provisional measures also can be adopted by FIUs themselves, or in some cases by financial institutions, even without the knowledge of the person affected by those measures and usually for a limited period of time.

#### 3.2 Provisional measures for cases with an international dimension

Regarding cases with an international dimension and when a country (referred to as the 'requesting country') requests the adoption of provisional measures from another country (referred to as the 'requested country'), the AML framework provides the following mechanisms as best practice:<sup>5</sup>

- The requested country has the possibility to take provisional measures, such as the freezing or

5 FATF, 'Best Practices Paper on Confiscation (Recommendations 4 and 38) and a Framework for Ongoing Work on Asset Recovery', October 2012, p. 5, par. 12. Available at

<http://www.fatfgafi.org/topics/fatfrecommendations/documents/bestpracticesonconfiscationrecommendations4and38andafameworkforongoingworkonassetrecovery.html>, viewed on 21 November 2014. According to the FATF Recommendation 38, those best practices should be applied during the process of mutual legal assistance (for more information on mutual legal assistance see 6.2.4 and chapter 4).



seizing of assets, on the basis of requests submitted prior to criminal charges having been laid against suspects in the requesting country. This is an early stage in the process of asset recovery in general.

- The freezing or seizing action can be enforced within a short timeframe, directly (by enforcing the foreign request itself) or indirectly (by obtaining a domestic order based on the evidence contained in the foreign request).
- The freeze/seizure can be kept in place until the requesting country has ruled upon the fate of the property concerned. Sufficient time is given to the requesting country to lead and conclude its criminal proceedings without the fear of losing the property.

Practitioners should rely on those measures that can be applied at an early stage in the investigative process and are of great value when there is fear that the property subject to confiscation can disappear/be moved to other foreign jurisdictions. It must be noted that in emergency situations some jurisdictions may also apply such measures following informal requests (such as requests between FIUs) when sufficient evidence is provided by the requesting authority (usually those informal requests will be followed by a formal mutual legal assistance [MLA] request).

### 3.3 Confiscation and the reversal of the burden of proof

Confiscation involves the actual change of ownership from the current owner to the state and is applicable to movable or immovable property, bank accounts and other financial products alike. Usually in order for assets to be confiscated, there must be a demonstration of their illicit origin.

However, the AML framework also provides for measures that require the offender to demonstrate the lawful origin of the property (to the extent that such a requirement is consistent with the principles of the country's national

#### DEFINITIONS - FREEZING, SEIZING, CONFISCATION

**Freezing** is a provisional measure applicable to bank accounts or other financial products that prevents the nominative owner of such products from moving, transferring or converting these assets.

**Seizing** is a provisional measure, applicable to movable or immovable property that prevents the nominative owner of such property from selling or transferring it, ideally for the duration of the criminal process.

**Confiscation** is a final measure applicable to movable or immovable property, bank accounts and other financial products alike that results in the actual change of ownership from the current owner to the state and is ordered at the very end of the criminal process.

law).<sup>6</sup> These measures are similar to provisions (such as those stemming from Article 20 of the UNCAC) for the criminalisation of unexplained wealth (or illicit enrichment).<sup>7</sup>

Practitioners should be aware that the burden of proof can be reversed in certain circumstances and, when allowed by law, if property is alleged to be liable to confiscation. In those cases, even if the prosecution still has the obligation to lay a factual basis for making the allegations, the offender will be called upon to explain the source of his wealth. The burden of proof is thereafter shifted to the offender, and he needs to demonstrate the lawful origin of the property. Below are some examples illustrating how the unlawful benefit acquired by an offender can be calculated thus requiring the offender

<sup>6</sup> FATF Recommendation 4.

<sup>7</sup> According to Article 20 of the UNCAC, illicit enrichment is a significant increase in the assets of a public official that he or she cannot reasonably explain in relation to his or her lawful income.

to prove its lawful origin:<sup>8</sup>

### Example 1

The unlawfully vested benefit is gained by a convicted person under three conditions:

- A person is convicted for a serious offence.<sup>9</sup>
- During the criminal investigation against such person, a criminal financial investigation commences.
- The criminal financial investigation shows that it was plausible that the offence for which the person was convicted, or other criminal offences, resulted in some way in the unlawful benefit – the calculation of that benefit can be based on a comparison of property or cash for a certain period (i.e. between the start of criminal conduct and the arrest for that conduct).<sup>10</sup>

### Example 2

The defendant has a criminal lifestyle from which he derives benefit. The criminal lifestyle occurs when:

- There is a lifestyle offence.
- It is part of a course of criminal conduct.
- It is an offence committed over a period of at least six months and the defendant has benefited from it – the court can calculate benefit based on his criminal lifestyle or based on the connection between the property/financial advantage obtained and the specific offence charged.

### 3.4 Non-conviction based confiscation

The AML framework provides also for non-conviction based confiscation, which enables practitioners to confiscate proceeds of a crime without the prior conviction of the offender. This measure allows taking action against property that is proved to be the proceeds of crime when it is not possible to convict the offender for a predicate offence.<sup>11</sup>

Confiscating laundered property, proceeds or instrumentalities without requiring a criminal conviction (non-conviction based confiscation or property confiscation or in rem-confiscation also known as civil asset forfeiture) can be applied mainly in the following circumstances:<sup>12</sup>

- When a perpetrator is unavailable by reason of death, flight, absence or is unknown;
- When a conviction cannot be obtained for procedural/technical reasons;
- When there is insufficient evidence to meet the criminal burden of proof but there is substantial evidence to prove that the proceeds were generated from the criminal activity;
- When a criminal investigation/prosecution is unrealistic or impossible;
- When the perpetrator has been acquitted of the predicate offence due to insufficient admissible evidence or failure to meet the burden of proof;
- When property was generated from other or related criminal activity of the convicted person; and
- When the perpetrator is immune from prosecution.

8 FATF, 'Best Practices Paper on Confiscation (Recommendations 4 and 38) and a Framework for Ongoing Work on Asset Recovery', op.cit., p.7, par. 23.

9 According to the Interpretive Note to the FATF Recommendation 3, the money laundering crime should apply to all serious offences.

10 See also chapter 3.

11 Interpretive Note to the FATF Recommendation 3, par. 4.

12 FATF 'Best Practices Paper on Confiscation (Recommendations 4 and 38) and a Framework for Ongoing Work on Asset Recovery', op.cit.,

In some jurisdictions, there are issues as to the extent to which the evidence/proof must relate back to the predicate offence, and there are noticeable legal and factual variances. In England and Wales, for example, prosecutors just have to show an 'irresistible inference' that the asset must have originated from a type of criminal offence, such as fraud, corruption or theft. The actual predicate offence does not have to be stipulated. Often this is proven by conducting a financial profile of the person in possession of the asset to show that the asset in question cannot have been obtained via any legal sources of income or capital, which in turn sets up the inference that it must have been generated by illegal means.

In certain other countries, however, some judges (and laws) appear to demand a more direct link to predicate offences – almost to the extent that this must be separately proven, which negates the whole point of the money laundering offence. This is a difficult area making some practitioners reluctant to charge money laundering offences unless there are also specific predicate offences.

### 3.5 Range of assets subject to freezing, seizing and confiscation

The AML framework explicitly describes the types of property and proceeds of crime that are subject to freezing, seizing and confiscation. These specifically include:<sup>13</sup>

- Property laundered;
- Proceeds from, or instrumentalities used in or intended for use in, money laundering or predicate offences;
- Property that is the proceeds of, or used in or intended or allocated for use in, the financing of terrorism, terrorist acts or terrorist organisations; and
- Property of corresponding value.

#### DEFINITION - NON-CONVICTION BASED CONFISCATION

**Non-conviction based confiscation** is confiscation through judicial procedures related to a criminal offence for which a criminal conviction is not required (Source: General glossary, the FATF Recommendations).

Practitioners should be aware that the range of such assets is very wide and includes not only property laundered or proceeds from money laundering and predicate offences but also property of corresponding value. This last aspect provides flexibility to freeze, seize or confiscate property, which may have been acquired by legal means when the illegally obtained property cannot be traced.

## 4. The use of AML preventive measures in asset tracing

The use of preventive measures in asset tracing is by and large a task to be implemented by private sector actors, such as financial institutions (FIs) and other reporting entities. Reporting entities are institutions that have a duty to report suspicious transactions but can also include other institutions, professions and individuals that are required to engage in the customer due diligence (CDD) and record keeping requirements. Whilst this might not be the focus of a practitioner's responsibility in tracing assets, it is still crucial to understand the specific preventive requirements in place in order to monitor and oversee the information provided by reporting entities as well as the kind of information a practitioner can expect to source from reporting entities. An in-depth knowledge of the AML preventive measures, particularly regarding CDD and record keeping requirements, is useful not only for an enhanced understanding of suspicious financial transaction identification, bank accounts and corporate vehicles, but also constructive cooperation and engagement with the private sector.

13 FATF Recommendation 4.

#### 4.1 Requirements in CDD and record keeping

FIs and designated non-financial businesses and professions (DNFBPs) are required to conduct CDD and keep records of the collected information. According to the FATF, DNFBPs include amongst others casinos, real estate agents, trust and company service providers, accountants and legal professionals when they engage in financial transactions.<sup>14</sup>

In most jurisdictions, reporting entities are required to conduct CDD when:

- Establishing a business relationship (e.g. opening a bank account);
- Carrying out occasional transactions above a designated threshold (thresholds may vary);
- Identifying a suspicion of money laundering or terrorist financing; or
- Doubting the veracity or adequacy of documents, data or information previously obtained for the purpose of CDD.<sup>15</sup>

CDD measures involve not only determining the customer’s identity but also ascertaining the intended nature and purpose of the business relationship. As an international standard, the CDD requires:

- Identifying the clients and verifying their identity on the basis of documents, data or information obtained from a reliable and independent source;
- Identifying the ‘beneficial owner’ involved in the business or transaction and verifying the identity, which includes understanding the ownership and control structure of a legal person, trust or similar arrangement;

- Obtaining information as to the purpose and intended nature of the business relationship; and
- Conducting ongoing due diligence with regard to the business relationship to ensure that the conducted transactions are consistent with the client’s profile and source of funds.<sup>16</sup>

Information on the nature of a business may serve to provide practitioners with critical evidence and leads during a criminal investigation. Information that might be relevant in order to understand the purpose and intended nature of the relationship may include some or all of the following:

- Details of the customer’s business or employment;
- The expected source and origin of the funds to be used in the relationship;
- Copies of recent and current financial statements;
- The nature and purpose of relationships between signatories and underlying beneficial owners; and
- The anticipated level and nature of the activity that is to be undertaken through the relationship.<sup>17</sup>

It must be noted that when clients are unable to provide standard verification documents due to lack of access to official documents or resources, then supervisory institutions and law enforcement may coordinate and establish alternative customer identification requirements<sup>18</sup>, such as letters from

<sup>14</sup> See FATF Recommendation 22 for complete list of DNFBPs.

<sup>15</sup> FATF Recommendation 10.

<sup>16</sup> FATF Recommendation 10.

<sup>17</sup> UK HM Revenue and Customs, ‘Anti-Money Laundering Guidance for Money Service Businesses’, 2010, p.18. Available at [http://www.hmrc.gov.uk/mlr/mlr8\\_msb.pdf](http://www.hmrc.gov.uk/mlr/mlr8_msb.pdf), viewed on 17 November 2014.

<sup>18</sup> Basel Institute on Governance ‘Working Paper No 14: Using Money Laundering Investigations to Fight Corruption in Developing Countries: Domestic Obstacles and Strategies to Overcome Them’, 2012, p. 22. Available at <https://www.baselgovernance.org/publications/370>, viewed on 12 November 2014.

an issuing authority or a driver's licence.<sup>19</sup>

One of the most critical elements for practitioners is the requirement (where applicable) of identifying the 'true beneficial owner'. Often clients are acting on behalf of another person or the true ownership is hidden behind corporate bodies or other entities.<sup>20</sup>

In addition to the CDD requirement, practitioners can also make use of the record keeping requirement that most jurisdictions have with respect to their reporting entities. The FATF stipulates that FIs and DNFBPs are required to maintain transaction records both domestically and internationally for at least five years. They are also required to keep all records that were obtained through CDD for at least five years after the business relationship ended. These records include copies of personal identification documents, account files, businesses associations and unusually large transactions, which allow for reconstructing the paper trail and may serve as evidence. Reporting entities should adequately maintain and record data in a consistent way and ideally in an electronic system. However, in several instances, records are available in paper format only making retrieval of information burdensome and time-consuming.

CDD information and record keeping are only useful if reporting entities effectively implement these requirements, and if there is enforcement of the requirements by the national supervisory bodies. Law enforcement and/or FIUs can contribute to more effective CDD and record keeping by enhancing inter-agency coordination and raising awareness within supervisory bodies and the private sector. Practitioners from law enforcement or FIUs can also play a useful role by coordinating with supervisory institutions in assisting with the drafting of guidelines and illustrating the importance of proper CDD and record keeping.

19 See for more information FATF 'Guidance on Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion', February 2013. Available at [http://www.fatf-gafi.org/media/fatf/documents/reports/AML\\_CFT\\_Measures\\_and\\_Financial\\_Inclusion\\_2013.pdf](http://www.fatf-gafi.org/media/fatf/documents/reports/AML_CFT_Measures_and_Financial_Inclusion_2013.pdf), viewed on 11 November 2014.

20 For more information see chapter 6.

#### DEFINITIONS

**Reporting entities** are institutions that have a duty to report suspicious transactions but also can include other institutions, professions and individuals that are required to engage in the customer due diligence and record keeping requirements.

**Financial institutions (FIs)** are those natural or legal persons who are engaged in conducting business for/on behalf of customers, such as acceptance of deposits, lending, financial leasing, money or value transfer services, issuing/managing means of payment, trading in: money market instruments, foreign exchange, transferable securities, commodity futures, changing money and currency, etc. (Source: FATF Recommendations, General Glossary).

**Designated non-financial businesses and professions (DNFBPs)** refers to casinos, real estate agents, dealers in precious metals, dealers in precious stones, lawyers, notaries, other legal professionals and accountants, trust and company service providers. (Source: FATF Recommendations, General Glossary).

**Customer due diligence (CDD)** are measures that FIs and DNFBPs are required to take in order to identify and verify the identity of their customers and beneficial owners and are categorised as 'enhanced' or 'simplified' according to the level of risk of money laundering or terrorist financing.

**Record keeping** is a process that FIs and DNFBPs should establish in order to maintain all necessary records on transactions for a period of at least five years.

## 4.2. Identification of politically exposed persons (PEPs)

Reporting entities are required to undertake additional due diligence measures in respect to customers who fall under the PEP category/definition. This requirement is useful for practitioners as they can derive more information from the reporting entities when the person involved in a case qualifies as a PEP. The FATF requires reporting entities to have in place an appropriate risk-management system to determine whether a customer or the beneficial owner is a PEP.

According to the FATF, PEPs are individuals who are or have been entrusted with prominent public functions in a foreign country (e.g. heads of state) including their family, close associates and businesses with which they have a relationship. Since February 2012, the definition of PEP has been broadened to include domestic PEPs and PEPs from international organisations as well.<sup>21</sup>

It is therefore essential to be familiar with the definition and coverage of national legislation regarding PEPs. Investigators conducting an analysis regarding a PEP can require additional information from reporting entities, such as networks of family members and close business associates. Several FIUs have the capacity to access and frequently use PEP (commercial) databases allowing the screening of individuals against PEPs or other risk factors.<sup>22</sup> However, during investigations it is essential to exercise due caution when screening a name against a list of PEPs or databases. For example, Internet searches and databases may not pick up on certain names or may exclude certain categories of PEPs. In addition, names may appear in certain languages only and inconsistent spelling variations may not show the desired results.

Screening names against a list of PEPs only is not sufficient

### DEFINITION - POLITICALLY EXPOSED PEOPLE (PEPS)

**Politically exposed persons (PEPs)** are individuals who are or have been entrusted with prominent public functions either domestically or by a foreign country, such as heads of state or government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. (Source: FATF Recommendations, General Glossary).

as a study of past international corruption cases has shown. Individual corrupt PEPs rarely act on their own and instead assign other less suspicious individuals or financial structures and gatekeepers to act on their behalf.<sup>23</sup> Often the use of front companies, lawyers, accountants and other professionals is employed to facilitate corruption and money laundering schemes. There are various financial vehicles or structures that can be utilised, which Chapter 6 will discuss in greater detail. The FATF, for instance, specifically requires life insurance companies to determine whether individuals who are beneficiaries of the proceeds of life insurance policies are PEPs.<sup>24</sup>

Where there is lack of adequate banking records and CCD information regarding PEPs, investigators and law enforcement face difficulties in obtaining such information and have to rely on alternative sources. An additional source of information that can be consulted in the event of an investigation is a jurisdiction's asset disclosures in which public officials (e.g. members of parliament, heads of state, cabinet members or senior civil servants) declare their financial and business assets/interests. Asset disclosure systems are beneficial in helping to assess the PEP customer's risk level and to ensure account activity is consistent with

<sup>21</sup> FATF Recommendation 12.

<sup>22</sup> Egmont Group White Paper, 'The Role of Financial Intelligence Units in Fighting Corruption and Recovering Stolen Assets', 2012. Available at <http://www.egmontgroup.org/news-and-events/news/2012/10/03/the-role-of-fius-in-fighting-corruption-and-recovering>, viewed on 12 November 2014.

<sup>23</sup> World Bank StAR, 'The Puppet Masters: How the Corrupt Use Legal Structures to Hide Stolen Assets and What To Do About It', 2011.

<sup>24</sup> FATF, 'FATF Guidance - Politically Exposed Persons (Recommendations 12 and 22)', June 2013, p. 12.

assets and values disclosed. It may even provide access to additional data, such as dates of birth and identification numbers, and insight into public functions. However, in many jurisdictions the legal requirement for asset disclosure does not exist or the accuracy of the database varies due to a lack of capacity and availability of sources of information.

#### 4.3. Targeted financial sanctions related to individuals and entities

Sanctions can be imposed against governments but also against targeted persons, entities and groups. Sanctions in general can include: diplomatic sanctions, trade sanctions, flight bans, financial sanctions, etc. Sanctions are included in specific lists (sanctions lists) issued multilaterally by the United Nations Security Council (UNSC) or the European Union (EU) but also autonomously by a country itself.

##### FINANCIAL SANCTIONS AGAINST DESIGNATED PERSONS (INDIVIDUALS OR

##### ENTITIES) INCLUDE TWO ELEMENTS:

- A prohibition on dealing with the funds or economic resources belonging to or owned, held or controlled by a designated person/entity; and
- A prohibition on making funds or economic resources available, directly or indirectly, to, or for the benefit of, a designated person/entity.<sup>25</sup>

Reporting entities are required to screen their existing and new customers against sanctions lists. The United Nations Security Council Sanctions Committees issue a Consolidated List, which includes all individuals and entities subject to

sanctions measures imposed by the Security Council.<sup>26</sup> The EU, as well as individual countries, implement the UNSC sanction lists and can also issue their own financial sanctions lists.<sup>27</sup>

Specifically, targeted financial sanctions relate to asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities.<sup>28</sup> Reporting entities are prohibited from carrying out transactions with the listed individuals and entities irrespective from suspicious activity. Whether reporting entities are required to file a suspicious transaction report (STR) depends on national regulatory requirements. The FIU or relevant regulatory body should issue guidance to reporting entities on how to treat individuals and entities on financial sanctions lists.

Practitioners can make use of such financial sanctions lists to identify sanctioned individuals/entities and should be aware that individuals who are listed on sanctions lists are not necessarily PEPs or been convicted of a crime. Asset freezing as a preventive measure aims to 'stop the flow of funds or other assets to terrorist groups; and the use of funds or other assets by terrorist groups'<sup>29</sup> or other sanctioned individuals/entities. In this case, the frozen assets cannot be further confiscated nor can they be returned to their country

26 See United Nations Security Council Sanctions Committees website available at: [http://www.un.org/sc/committees/list\\_compend.shtml](http://www.un.org/sc/committees/list_compend.shtml), viewed on 12 November 2014.

27 The United Kingdom Home Treasury (HM Treasury) operates a range of financial sanctions. These may follow action at the United Nations, European or domestic (UK) level and include asset freezing measures. Similarly, the United States (US) issues financial country sanctions through their Office of Foreign Assets Control - Sanctions Programs and Information (OFAC). OFAC also publishes a list of individuals and companies whose assets must be blocked, and US persons are generally prohibited from dealing with them. The EU also maintains a list of persons and entities that are subject to financial restrictive measures, such as asset freeze. See for an updated list: [http://eeas.europa.eu/cfsp/sanctions/consol-list/index\\_en.htm](http://eeas.europa.eu/cfsp/sanctions/consol-list/index_en.htm).

28 FATF, 'International Best Practices - Targeted Financial Sanctions Related to Terrorism and Terrorist Financing (Recommendation 6)', 2013, p. 3, footnote 2.

29 Interpretative Note to the FATF Recommendation 6, par. 2.

25 HM Treasury - Financial Sanctions Frequently Asked Questions (FAQ). Available at [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/302397/August\\_2013\\_version\\_-\\_amended.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/302397/August_2013_version_-_amended.pdf), viewed on 30 October 2014.

of origin without due process and judicial proceedings.

## 5. The role of FIUs in asset tracing

The FIUs are national agencies that receive and analyse STRs or suspicious activity reports (SARs) as well as any other information related to money laundering, predicate offences or terrorist financing. They furthermore disseminate the results of that analysis to their counterparts (mainly law enforcement, prosecutors and foreign FIUs).<sup>30</sup>

The FIU is a crucial actor in the AML framework and the process of tracing illegal assets, as it can act as an interface between the private sector and LEAs, enabling the flow of relevant financial information.<sup>31</sup>

The role of FIUs in the asset tracing process depends on the following:

- The powers of action entrusted to them as well as their characteristics according to their type;
- The amount and quality of the information they receive; and
- The effective handling/analysis of sensitive and, most of the time, confidential information accumulated.

### 5.1 Types of FIUs

When practitioners are keen to get an FIU involved in an asset recovery case or receive information from it, they should first be aware of the powers of action delegated to

#### DEFINITION - FINANCIAL INTELLIGENCE UNIT

**Financial Intelligence Unit (FIU)** is a national agency that receives and analyses suspicious transaction reports (STRs) or suspicious activity reports (SARs) as well as any other information related to money laundering, predicate offences or terrorist financing, and furthermore disseminates the results of the analysis to its counterparts.

the particular FIU and its characteristics.

These powers/characteristics, but also constraints, are related to the type of FIU: administrative, judicial/prosecutorial, law enforcement, hybrid, and are summarised more specifically on the next page.<sup>32</sup>

<sup>30</sup> FATF Recommendation 29.

<sup>31</sup> EGMONT Group, 'The Role of Financial Intelligence Units in Fighting Corruption and Recovering Stolen Assets, An Egmont Group White Paper', October 2012, Executive Summary, p. 1. Available at <http://www.egmontgroup.org/news-and-events/news/2012/10/03/the-role-of-fi-us-in-fighting-corruption-and-recovering>, viewed on 21 November 2014.

<sup>32</sup> International Monetary Fund/World Bank, 'Financial Intelligence Units An Overview', July 2004, p. 9-17. Available at <http://www.imf.org/external/pubs/ft/FIU/fiu.pdf>, viewed on 21 November 2014.



Type of FIU	Powers/Characteristics	Constraints
<b>Administrative</b>	<ul style="list-style-type: none"> <li>• Acts as intermediary between the reporting entities and the LEAs (being a natural interlocutor)</li> <li>• Reporting entities are more willing to give information when dissemination will be limited to money laundering/terrorist financing issues and included in the FIU's analysis/report</li> <li>• Neutral, technical and specialised intermediary</li> <li>• Usually placed in a regulatory agency</li> <li>• Information can be exchanged with all types of FIUs</li> </ul>	<ul style="list-style-type: none"> <li>• Delays in applying law enforcement measures</li> <li>• No direct powers to obtain evidence</li> <li>• Subject to direct supervision from political authorities (unless truly independent)</li> </ul>
<b>Judicial/Prosecutorial</b>	<ul style="list-style-type: none"> <li>• Works best in systems with strong banking secrecy laws</li> <li>• Within the judicial system</li> <li>• Can exercise judicial powers</li> <li>• Higher degree of independence from political will</li> <li>• Information is brought directly to an agency authorised to investigate/prosecute</li> <li>• Freezing/seizing and other judiciary powers can be immediately exercised</li> </ul>	<ul style="list-style-type: none"> <li>• More focus on investigations than prevention</li> <li>• Not a natural interlocutor for reporting entities/takes time to establish trust</li> <li>• Limited information received as it does not receive data on currency transactions above a fixed amount</li> <li>• Difficulty in exchanging information with non-judicial/prosecutorial FIUs</li> </ul>
<b>Law Enforcement</b>	<ul style="list-style-type: none"> <li>• Within an existing infrastructure/agency;</li> <li>• Maximum law enforcement use of financial information;</li> <li>• Quick law enforcement response to illegal activities;</li> <li>• Freezing/seizing in timely manner;</li> <li>• Information can be exchanged through the extensive network of international networks;</li> <li>• Easy access to criminal intelligence.</li> </ul>	<ul style="list-style-type: none"> <li>• More focus on investigations than prevention;</li> <li>• Not a natural interlocutor for reporting entities/takes time to establish trust;</li> <li>• Usually does not receive data on currency transactions above a fixed amount;</li> <li>• To access the financial organisations' data may first require the initiation of a formal investigation;</li> <li>• Reporting institutions will be aware of the fact that information given could be used in the investigation of any crime.</li> </ul>
<b>Hybrid</b>	<ul style="list-style-type: none"> <li>• Combines powers of the above types.</li> </ul>	

## 5.2 Reporting obligations and information received by FIUs

In the asset tracing process, valuable information for practitioners can be derived from the STRs or SARs or other disclosures filed with the FIU.

LEAs and FIUs usually receive a large amount of data from STRs and other disclosures made.<sup>33</sup> At the same time, reporting entities may file an official report with respect to a suspicious activity/transaction without having any knowledge or suspicion of a specific offence. The reporting mechanism often operates as a gateway to discovering illegal activities/predicate offences.

The effectiveness of the STRs/SARs/disclosures in the asset tracing process mainly depends on the following:

- The content and details of the reports; and
- The identification and actual filing of all suspicious transactions by the reporting entities (FIs and DNFBPs).

### 5.2.1 Content of the suspicious transaction report (STR)

FIs and DNFBPs are obliged to file a STR or SAR with the FIU when they suspect, or have reasonable grounds to suspect, that funds are the proceeds of a criminal activity or are related to terrorism financing.<sup>34</sup> These reports should contain all relevant information with regard to the person(s) related to the suspected activity/transaction as well as the activity/transaction itself. The more information provided, the more effective the resulting investigation of the suspicious activity/transaction by the FIU and, subsequently, the tracing of the assets.

Most FIUs usually have prepared forms or templates for filing an STR/SAR available on their websites. They may also request additional information from the reporting entities, including information that reporting entities are required to maintain pursuant to relevant FATF Recommendations (CDD and record keeping) and their national law.<sup>35</sup>

In general, the following information needs to be included in the STRs/SARs as a minimum and supported by relevant documentation. Practitioners should be aware that this information can be derived from the STRs/SARs (see next page):

### 5.2.2 How to achieve the most effective cooperation between FIUs and reporting entities in filing STR reports

FIUs can analyse suspicious transactions provided that reporting entities comply with their obligation to file the respective reports in practice. FIUs can raise awareness about the importance of submitting STRs/SARs and inform reporting entities about their reporting obligations. The most effective cooperation between FIUs and reporting entities can be achieved through the following:

- **Trust.** There should be a relationship of trust between the FIU and the reporting entities through regular cooperation and communication. When the reporting entity feels that information shared with the FIU will be handled confidentially and action taken accordingly, it will be keen to file more reports.
- **Supervision.** FIs and DNFBPs are effectively supervised and regulated through relevant competent authorities and/or supervisory bodies or self-regulatory bodies. Supervisors should apply a risk-based approach: i) in allocating their supervisory resources based on their understanding of risks (present in the country and associated with the products, services and customers); and ii) when supervising DNFBPs, by taking

33 For data sources and types of information see FATF, 'Operational Issues Financial Investigations Guidance', June 2012, p. 17-19. Available at <http://www.fatf-gafi.org/topics/methodsandtrends/documents/operationalissues-financialinvestigationguidance.html>, viewed on 21 November 2014.

34 FATF Recommendations 20 and 23.

35 FATF Recommendation 29 and Interpretative Note to the FATF Recommendation 29, par. 5.

Type of information	Included in the STR/SAR	Supporting documents
<b>Identity of the subject(s) (natural persons)</b>	Name, address, phone number, email, date of birth (DOB), place of birth (POB), citizenship, tax identification number, profession	Copy of identification documents, passport, any other personal identification document
<b>Identity of the subject(s) (legal persons)</b>	Legal form, legal name, address, phone number, email, tax identification number, legal representatives, shareholders or partners, or beneficial owners (up to natural person)	Certificate of incorporation, certificate of good standing, partnership agreement, trust instrument (e.g. deed of trust, legal representation documents, other documents from reliable source)
<b>Related persons (natural/legal) to the subject(s) and known to the reporting entity</b>	See above	See above
<b>Financial transactions</b>	Amounts (debits, credits), accounts, counterparts	Copy of bank records
<b>Wire transfer</b>	Payers/beneficiaries	Copy of wire transfers
<b>Activity conducted (other than financial)</b>	Nature, purpose, description, reasons for being suspicious	Business correspondence, any other related documents
<b>Suspected predicate offence in relation to ML/TF</b>	Description or indication of typology related to ML/TF	
<b>Geographical indication of the transaction/activity</b>	Description of the geographical area involved in the suspected transaction/activity	
<b>Actions taken by the reporting entity</b>	Description, commentary and justification of the suspected or unusual transaction/activity  Results of investigation and further actions taken  Description of the cooperation/relationship with the subject and the extent/scope of the subject's activities	Any supporting documentation

into consideration their money laundering/terrorist financing risk profile and the degree of discretion allowed to them under the risk-based approach.<sup>36</sup> These supervisors have considerable influence on the behaviour of FIs. Once effective supervision has been established, supervisors can work closely with practitioners by providing them with information on constraints and challenges they face with reporting entities in order for the latter to be reminded of their obligations.<sup>37</sup>

- **Sanctions.** Dissuasive, proportionate and effective sanctions are imposed on FIs and DNFBPs as well as their directors and senior management for not reporting. Sanctions can be civil, administrative or criminal.<sup>38</sup> Most of the time it is not the severity of the punishment that operates as a deterrent to crime but an awareness that the illegal act will definitely be punished.

On the criminal side, in particular, it is extremely important to note that an FI or DNFBP (in countries where there is criminal liability for legal persons) and their directors and senior management can be accused of money laundering by acting (or aiding, abetting, facilitating, counselling, etc.) in the process when they fail to meet their reporting obligations and a money laundering offence has been committed.

### 5.3 The role of the FIU in financial investigations and adding value to data

Following receipt by the FIU of STRs/SARs or other disclosures, the FIU should try to identify potential cases of money laundering or terrorism financing by analysing the information received, requesting additional information

<sup>36</sup> FATF Recommendation 28.

<sup>37</sup> International Centre for Asset Recovery, 'Tracing Stolen Assets, A Practitioner's Handbook', 2009, p. 68. Available at [https://www.baselgovernance.org/sites/collective.localhost/files/publications/asset-tracing\\_web-version\\_eng.pdf](https://www.baselgovernance.org/sites/collective.localhost/files/publications/asset-tracing_web-version_eng.pdf), viewed on 21 November 2014.

<sup>38</sup> FATF Recommendation 35.

where needed, using various open and closed database sources and, depending on its powers, applying various investigative techniques. When the amount of information received is very large, there should be rules for prioritising the information based on pre-established criteria, such as significance, investigative priorities, national strategies, etc.

#### 5.3.1 Financial investigations

Generally, AML investigations may be initiated based on the following two scenarios:

- When money laundering and predicate offences have been committed ➡ trace the illegally obtained assets and take respective measures.
- When there is only information in relation to suspicious transactions/activities performed ➡ discover any offences committed and thereafter trace the illegally obtained assets and take respective measures.

The financial investigation can be an important tool in the process of discovering the commission of an offence: by following the trail of the suspicious transactions and any other information, investigators can uncover the commission of a specific predicate offence.

At the same time, practitioners should be aware that the AML framework emphasises the importance of conducting parallel investigations, meaning simultaneous investigations of the predicate and the money laundering offences. The financial investigation of the predicate offence, which is often proactive (in relation to the tracing of assets) and takes place at an early stage of the process, is extremely valuable and effective as it identifies the proceeds of crimes to be seized/restrained and can prevent the assets from disappearing and infiltrating the legal economy.<sup>39</sup>

<sup>39</sup> FATF 'Operational Issues Financial Investigations Guidance', op. cit., p. 9, par. 22.

### 5.3.2 The process of analysis

The scope of the analysis is to integrate and interpret all information available and then convert such information into intelligence. Figure 2 briefly describes the mechanism of analysis within an FIU.

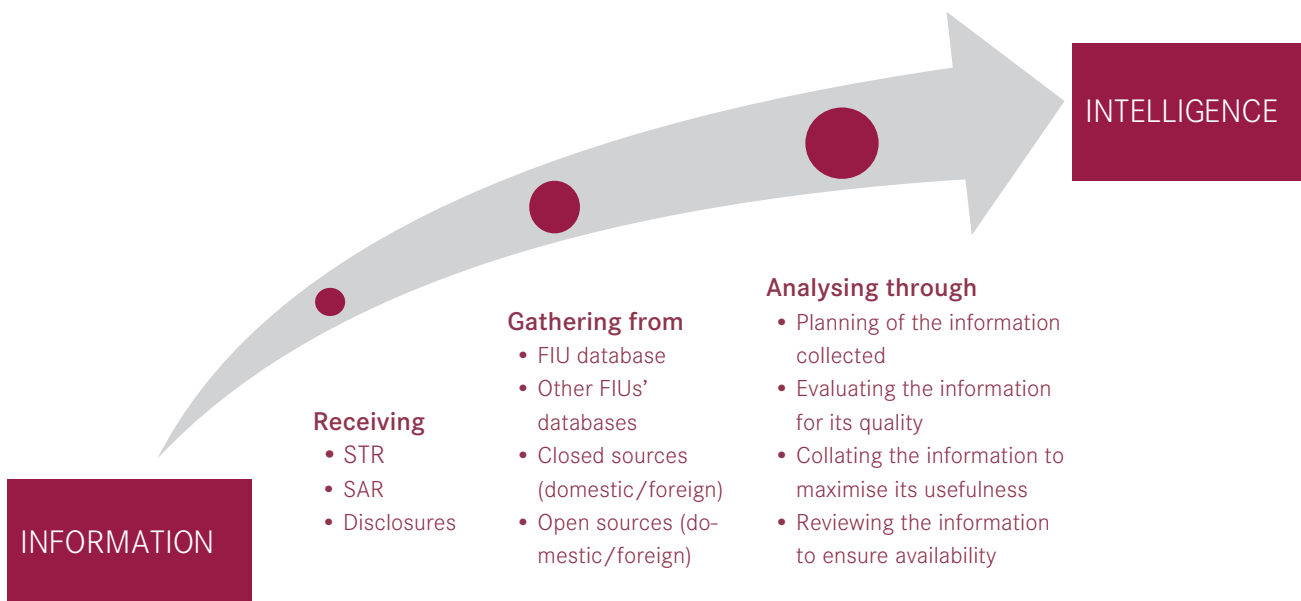


Figure 2 - The process of converting information into intelligence

Usually, the FIU conducts two types of analysis: operational and strategic. The basic characteristics of the two types of analysis can be summarised below.<sup>40</sup>

	Operational analysis	Strategic analysis
<b>Scope</b>	<ul style="list-style-type: none"> <li>Identify specific targets (persons, assets, criminal networks, etc.), follow the trail of particular activities/transactions and determine links between the targets and proceeds of crime, money laundering/terrorist financing and predicate offences.</li> </ul>	<ul style="list-style-type: none"> <li>Identify money laundering and terrorist financing related trends and patterns and develop strategic intelligence knowledge for money laundering/terrorist financing and other threats to a country;</li> <li>Provide input for policy formulation and setting operational priorities.</li> </ul>
<b>Major components</b>	<ul style="list-style-type: none"> <li>Matching with predefined lists;</li> <li>Identifying all reports that relate to the same entity;</li> <li>Capturing all possible relationships across entities;</li> <li>Analysing relationships to establish the closely related ones.</li> </ul>	<ul style="list-style-type: none"> <li>Examining data for patterns;</li> <li>Identifying connections/links between pieces of information;</li> <li>Developing inferences;</li> <li>Constructing arguments leading to inferences.</li> </ul>
<b>Products</b>	<ul style="list-style-type: none"> <li>Report on the findings for the specific targets.</li> </ul>	<ul style="list-style-type: none"> <li>Typologies and trends;</li> <li>Patterns;</li> <li>Geographical/regional analysis;</li> <li>Behavioural analysis;</li> <li>Activity analysis.</li> </ul>

<sup>40</sup> Interpretative Note to FATF Recommendation 29, par. 3 and EGMONT, 'Egmont Group of Financial Intelligence Units, Operational Guidance for FIU Activities and the Exchange of Information', July 2013, p. 9-10. Available at [www.egmontgroup.org/library/download/292](http://www.egmontgroup.org/library/download/292), viewed on 21 November 2014.

Following the analysis of the information received as described above, usually a report is prepared where the findings and all intelligence is gathered. Those reports may contain important information for practitioners regarding illegally obtained assets and individuals linked to them. This information can be used during ongoing investigations in order for practitioners to take proactive action and prevent the disappearance of the assets.

#### **5.4 Dissemination of information to other authorities**

What a practitioner should expect to receive from an FIU depends on whether the FIU is permitted to disseminate information, what information it is permitted to disseminate and to whom according to the national law and type of FIU. Generally the FIU should be able to disseminate, spontaneously or upon request, information and the results of its analysis to relevant competent authorities through dedicated, secure and protected channels.

When an FIU has information that might be useful to another FIU, it should consider forwarding it spontaneously without prior request in order to assist the receiving FIU in initiating its own investigation.

However, when information is being requested, then the decision regarding what information should be provided in response to that request remains with the FIU.<sup>41</sup>

Usually, the STR/SAR itself is not shared with other authorities due to the duty of confidentiality applicable to FIUs regarding information they receive. The FIU can disseminate spontaneously the reports where intelligence is gathered as well as other information when requested. The other authorities have a duty to maintain the confidentiality of the information provided and not to disclose it without prior written consent.

---

<sup>41</sup> Interpretative Note to the FATF Recommendation 29, par. 4.

## 6. The role of national and international cooperation in asset tracing

### 6.1 Cooperation at national level



#### 6.1.1 Information sharing

Practitioners need to rely on effective inter-agency cooperation to gather information and share intelligence. One of the prerequisites in this regard is an element of trust between authorities and various law enforcement entities. Information related to AML is sensitive as it allows access by authorities to an individual's financial information.<sup>42</sup>

The cooperation at national level can provide practitioners with information from a number of additional resources (besides the information received from FIs (STRs)), which can be extremely valuable during an investigation. The list below contains a number of resources and databases that could be available to practitioners when cooperating with the respective agencies in possession thereof:

- Land registry /registry of real estate;
- Investigative journalists' databases;<sup>43</sup>
- Criminal records and intelligence;
- Drug-related databases;
- Customs and border control databases;
- Civil and criminal court records;
- Licensing records;
- Probate and death records;
- Commercial registry records;
- Tax records/files; and
- Immigration and naturalisation records.

#### 6.1.2 Creating multidisciplinary groups

Investigative and prosecutorial powers may be divided amongst various authorities, emphasising the need to have formalised coordination mechanisms, which enable

42 See more on trust as a challenge in AML measures: Basel Institute on Governance 'Working Paper No 14: Using Money Laundering Investigations to Fight Corruption in Developing Countries: Domestic Obstacles and Strategies to Overcome Them', 2012.

43 See for more information the International Consortium of Investigative Journalists (ICIJ) available at <http://www.icij.org/offshore/secret-files-expose-offshores-global-impact>, and the Investigative Dashboard by OCCRP available at <https://investigativedashboard.org/>, viewed on 6 November 2014.



authorities to develop and implement a coordinated money laundering investigation. Creating a multidisciplinary group or task force, particularly in large, complex financial investigation cases, ensures effective cooperation between investigation, prosecution and confiscation authorities. A coordinated approach or a multidisciplinary group may comprise representatives of several agencies, such as a regulatory authority, the FIU, a tax authority, an auditing agency, the office of an inspector general, customs and border control, and even the private sector.

A less formal way to make coordination happen would be through MoUs in order to exchange information and create

joint investigative units. Even though MoUs are a weaker instrument than legislation, they promote and enhance cooperation and data sharing for the benefit of money laundering investigations.

## 6.2 Cooperation at international level

There is no doubt that international cooperation is essential for a successful investigation into money laundering and tracing stolen assets. As chapter 2 has outlined, a joint investigation with international counterparts should be both well-planned and part of an overall investigative strategy.



### 6.2.1 Contacting liaison officers

The practitioner should review his domestic case strategy before turning to international counterparts. Then, he can review what prior efforts have been made to cooperate internationally, what information already has been requested and what information already has been made available. One of the first steps is to request informal investigative assistance from the liaison officer.

### 6.2.2 Exchanging information through various channels

Exchange of information can take place through various channels and through a number of practitioners' networks available, such as the Interpol Global Focal Point Network<sup>44</sup> and the Camden Asset Recovery Inter-Agency Network (CARIN).<sup>45</sup> These networks can facilitate informal investigative assistance and cooperation. They may facilitate personal connections with foreign counterparts, which are also important to successful investigations, as they help reduce delays, particularly where differences in terminology and legal systems may lead to misunderstandings. Direct contact via phone, email or face-to-face meetings with foreign counterparts may speed up long procedures with fewer formalities and lead to a better understanding of specific requirements or conditions in foreign jurisdictions.<sup>46</sup>

### 6.2.3 Contacting foreign FIUs

The exchange of information between national FIUs can be made through various secure channels, such as the FIU Net and EGMONT Secure Web. Usually FIUs sign bilateral or multilateral MoUs with their counterparts that clearly

44 Interpol Global Focal Point Network, available at <http://www.interpol.int/Crime-areas/Corruption/International-asset-recovery>, viewed on 19 November 2014.

45 See for more information about CARIN <https://www.europol.europa.eu/content/publication/camden-asset-recovery-inter-agency-network-carin-manual-1665>, viewed on 19 November 2014.

46 FATF, 'Operational Issues Financial Investigations Guidance', June 2012. Available at <http://www.fatf-gafi.org/topics/methodsandtrends/documents/operationalissues-financialinvestigationguidance.html>, viewed on 21 November 2014.

#### DEFINITION - MUTUAL LEGAL ASSISTANCE (MLA)

**Mutual legal assistance (MLA)** is a formal mechanism for exchanging information, requesting and obtaining evidence for criminal investigations and prosecutions through a proper legal channel called a mutual legal assistance request (MLAR).

define the method of cooperation and address confidentiality issues.

The cooperation between FIUs provides intelligence in an informal way and most of the time at an early stage of the investigative process. Specifically, in the process of tracing illegal assets, practitioners should be aware that the AML framework requires countries to enact national measures related to taking expeditious action in response to requests by foreign countries for the identification of property subject to confiscation.<sup>47</sup> Those measures aim to secure and prevent the disappearance of the illegally obtained property (see also above 3.1).

When contacting foreign FIUs to request further information, a proper justification should be given to the requested FIUs. For example, the fact that individuals are on a sanction list does not automatically permit an FIU to share all data related to the sanctioned individuals.

### 6.2.4 The process of MLA and reverse MLA

MLA is a key mechanism when requesting further information for an investigation and/or obtaining evidence that is admissible in court. In the latter case, practitioners must make use of the applicable international arrangements, which may be based on reciprocity, MoUs, bilateral or multilateral arrangements. Practitioners should also be aware that the AML framework allows a country to open an investigation based on information received by a foreign country through

47 FATF Recommendation 38.

a formal MLA request.<sup>48</sup>

Take the following example: Country A sends an MLA request to Country B for information with respect to a corruption investigation into one of its national public officials where the corrupt activity is suspected to have been committed in Country A and the proceeds thereof laundered in Country B. Country B can use its own AML framework to open an investigation against individuals or financial institutions where the assets are believed to be located. This procedure may lead the investigator in Country B to a situation where he would have to request information from Country A. To substantiate the latter MLA request, the investigator would have to consider offering information to Country A where the predicate offence had its origin.

Through this process both countries can benefit and exchange information, and, particularly, the country where the predicate offence was committed (Country A) can gather important elements to bolster its investigation.<sup>49</sup>

---

48 For details on drafting and submitting an MLA request see chapter 4.

49 International Centre for Asset Recovery, 'Tracing Stolen Assets, A Practitioner's Handbook', 2009. Available at [https://www.baselgovernance.org/sites/collective.localhost/files/publications/asset-tracing\\_web-version\\_eng.pdf](https://www.baselgovernance.org/sites/collective.localhost/files/publications/asset-tracing_web-version_eng.pdf), viewed on 21 November 2014.



# 6. The use of corporate vehicles to conceal illegal assets

Phyllis Atkinson

1. Introduction	95
2. What is a corporate vehicle?	96
2.1 Meaning of offshore	97
2.2 Role of trust and corporate services providers	98
3. Beneficial ownership	99
4. Typical corporate vehicles used for criminal purposes	99
4.1 Shell companies	100
4.2 Shelf companies	102
4.3 Trusts	104
5. Establishing control and benefit	108
5.1 International cooperation	109
5.2 Relevant documentation/information	110



## 1. Introduction

As criminals become more aware of the opportunities afforded by the global economy to commit increasingly ingenious crimes, they develop increasingly more sophisticated ways of concealing their illicit gains. Money laundering is the process through which illegally obtained proceeds of a criminal activity are converted or transformed into ostensibly legitimate money or other assets in order to conceal or disguise their illicit origin or source. It is a crime that always requires the commission (but not conviction) of another crime, a predicate offence. Criminals and organised crime syndicates keep the profits of their crime by inventing money laundering schemes aimed at creating a 'disconnect' between themselves and the proceeds of their criminal activities. These disconnects ultimately facilitate a criminal's safe enjoyment of the fruits of his crime.

Sophisticated money laundering schemes frequently involve complex webs of transactions and structures, which offer disguise, concealment and anonymity, and transcend international borders. By laundering the proceeds of crime, dirty money is often provided with the semblance of a legitimate source through the use of corporate vehicles. For example, funds can be moved through various bank accounts, mostly belonging to several different corporate vehicles in multiple jurisdictions, thus obscuring the audit trail and severing the link with the original crime. The criminal later benefits from such funds, which ultimately appear to emanate from a legitimate source.<sup>1</sup>

In many instances, the criminal does not act alone but

1 Take the following example: X receives a bribe in return for awarding a contract to Company A, which is owned by Y. Company A transfers the funds to Company B, a mere shell company that is also owned by Y, for services rendered. The money is later withdrawn from Company B and placed in an investment portfolio with a stockbroker under the name of W, a nominee of X, who opens an account with the same stockbroker in the name of Company D, a shell company belonging to X's son. The money in W's account is used to purchase shares in the open market, which are later sold to Company D. Company D sells the shares at a higher price and uses the profits to open a fixed deposit and later purchase an insurance policy in X's name.

engages the services of professionals to design complex structures to achieve his objectives.<sup>2</sup>

Corporate vehicles, including corporations, trusts, foundations, partnerships with limited liability and similar structures, have become an integral and indispensable component of the modern global financial landscape. However, as the Financial Action Task Force (FATF)<sup>3</sup> emphasised, they may be exploited for unlawful purposes, including money laundering.<sup>4</sup> As banks and other financial institutions put money laundering defences in place, criminals respond by misusing corporate vehicles, and those who provide trust and company services, to disguise and convert their criminal proceeds before they enter the traditional financial system. The criminal's choice of money laundering vehicles that mask illegal activities is limited only by his creativity.

The success of public corruption, money laundering and most financial crime investigations depends largely upon the ability of the criminal investigator to track the ownership trail of money and other assets, which leads away from the crime or the criminal to both domestic and offshore destinations.

**It is essential to be able to link the perpetrator to the beneficial ownership of such assets.**

The practitioner should therefore develop an understanding of the types of assistance and structures commonly provided

- 
- 2 See chapter 5 on the anti-money laundering framework and the use of various aspects thereof to trace illegally obtained assets.
  - 3 FATF is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.
  - 4 FATF, 'The Misuse of Corporate Vehicles, Including Trust and Company Service Providers', 13 October 2006, Executive Summary, p. i, para. 1, viewed on 16 June 2014. Available at [http://www.fatfgafi.org/media/fatf/documents/recommendations/pdfs/FATF\\_Recommendations.pdf](http://www.fatfgafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf).

by trust and company service providers (TCSPs)<sup>5</sup> and other professionals being used as gateways through which criminals disguise the illegal origins of their assets. It is essential to understand the manner in which a veneer of respectability is obtained and secrecy exploited by engaging professional service providers, and how corporate vehicles are manipulated and misused in the process.

This chapter will explain the meaning of ‘corporate vehicle’ and other related concepts, such as beneficial ownership, and the role of corporate service providers before focusing on the most common types of corporate vehicles used for illicit purposes.

## 2. What is a corporate vehicle?

By understanding what is meant by a corporate vehicle (also commonly referred to as a structure), particularly in the context of offshore jurisdictions, practitioners assist in dispelling the mystique often associated with criminal investigations involving such structures. They need to enhance their knowledge of the different kinds of corporate vehicles available in foreign countries and their licit and illicit uses to increase the chances of following the money trail in major corruption and money laundering cases.

5 In the FATF report, ‘The Misuse of Corporate Vehicles, Including Trust and Company Service Providers’, op. cit., p.28, trust and company service provider (TCSP) has the same meaning as in the glossary attached to the FATF Forty Recommendations. It ‘refers to any person or business that provides any of the following services to third parties:

- acting as a formation agent of legal persons;
- acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
- providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangements;
- acting as (or arranging for another person to act as) a trustee of an express trust; and
- acting as (or arranging for another person to act as) a nominee shareholder for another person’.

The following words and/or terminology are pertinent to an understanding of corporate vehicles:

‘Corporate’ means relating to a large company or group, or a corporate company or group.

A company is ‘a legal entity, allowed by legislation, which permits a group of people, as shareholders, to apply to the government for an independent organisation to be created, which can then focus on pursuing set objectives, and empowered with legal rights which are usually only reserved for individuals, such as to sue and be sued, own property, hire employees or loan and borrow money’.<sup>6</sup>

A company (also referred to as a corporation in some jurisdictions) is owned by its shareholders who share in profits and losses generated through its operations. Therefore, the beneficial owner of a company or corporation is, generally speaking, the shareholder, i.e. the person (individual or corporate) in whose name shares in a particular company are registered. However, in some situations the shareholder may hold shares for the benefit and on behalf of another person. Such a shareholder would be called a ‘nominee shareholder’ and the other person – who would be the real owner of the shares – is the beneficial owner of such shares. In other words, the beneficial owner is the person who is the real *de facto* owner of the shares and is entitled to all gains, profits and benefits accruing to such shares. The beneficial owner would also be the one who decides on the ultimate sale or disposition of shares. Accordingly, not all beneficial owners are shareholders and not all shareholders are beneficial owners – while, certainly, it is also possible that both are the same person.

Companies or corporations are required to meet certain legal requirements in order to receive recognition as entities

6 Available at <http://www.duhaime.org/LegalDictionary/C/Company.aspx>, viewed on 23 October 2014.



separate from their owners.<sup>7</sup> From the juristic point of view, a company is a separate, legally recognised corporate entity created by means of a fictional veil between the company and its members, which shields the people behind the company or corporation from personal liability. Companies or corporations have distinct characteristics, such as a legal existence that allows them to buy, sell, own or enter into a contract. They can sue other persons and entities, and be sued by them. Companies or corporations also have limited liability and continuity of existence, i.e. they can live beyond the life spans and capacity of their owners because their ownership can be transferred through a sale or gift of shares.<sup>8</sup>

The corporate veil is pierced when, firstly, it is established that the individuals behind the company or corporation dominate the entity's finances and business practices to the extent that the corporate entity no longer has a separate will or existence. And, secondly, the control has resulted in a criminal, dishonest or unjust act which caused injury or unjust loss.

Corporate vehicles are 'legal entities through which a wide variety of commercial activities are conducted and assets are held. They are the basis of most commercial and entrepreneurial activities in market-based economies'.<sup>9</sup>

They play an essential role in the global economic system but may, under certain conditions, be used for illicit purposes, including money laundering, bribery/corruption, misappropriation of public funds, hiding and shielding

assets from creditors, illicit tax practices, market fraud, circumvention of disclosure requirements and other forms of unlawful behaviour.

The crux of the issue for any practitioner faced with unravelling the 'beneficial owner' of the corporate vehicle is the ability to 'see through' the corporate veil provided by the structure to identify the controlling party, commonly referred to as the beneficial owner (defined in paragraph 1.3 below).

## 2.1 Meaning of offshore

Although the term 'offshore' is not defined by the FATF, in the context of corporate vehicles it refers to something located or based outside of one's national boundaries, i.e. in a foreign country. It is commonly used to describe foreign banks, trusts, corporations, investments and deposits. Although a company may legitimately move offshore for the purpose of tax avoidance or to enjoy relaxed regulations, offshore financial institutions can also be used for illicit purposes, such as money laundering and tax evasion. Offshore vehicles or structures formed in offshore financial centres (OFCs) - those jurisdictions whose corporate vehicles are primarily used by non-residents - usually include companies, partnerships or trusts that are located, established or registered offshore.

According to the Financial Stability Forum (FSF) Working Group on Offshore Financial Centres,<sup>10</sup> OFCs are not easily defined but 'can be characterised as jurisdictions that attract a high level of non-resident activity. Traditionally, the term has implied some or all of the following (but not all OFCs operate this way):

- Low or no taxes on business or investment income;
- No withholding taxes;

<sup>7</sup> It must be born in mind that although a trust (to be discussed in greater detail below) also qualifies as a corporate vehicle, it does not have a separate legal personality like a company or corporation.

<sup>8</sup> Available at <http://www.businessdictionary.com/definition/corporation.html#ixzz3F01CPCEU>, viewed on 22 October 2014.

<sup>9</sup> The term 'corporate vehicle' is defined by the FATF as having the same meaning as in the 2001 Organisation for Economic Co-operation and Development (OECD) Report 'Behind the Corporate Veil - Using Corporate Entities for Illicit Purposes', and it embraces corporations, trusts, partnerships with limited liability characteristics, foundations, etc. Available at <http://www.oecd.org/daf/ca/43703185.pdf>.

<sup>10</sup> Financial Stability Forum, Report of the Working Group on Offshore Financial Centres, 5 April 2000 ('FSF OFC Report'), p. 9, Box 2, viewed on 23 July 2014. Available at [http://www.financialstabilityboard.org/publications/r\\_0004b.pdf](http://www.financialstabilityboard.org/publications/r_0004b.pdf).

- Light and flexible incorporation and licensing regime;
  - Light and flexible supervisory regime;
  - Flexible use of trusts and other special corporate vehicles;
  - No need for financial institutions and/or corporate structures to have a physical presence;
  - An inappropriately high level of client confidentiality based on impenetrable secrecy laws; and
  - Unavailability of similar incentives to residents’.
- Offshore company;<sup>12</sup>
  - Offshore trust;<sup>13</sup>
  - Offshore partnership; and<sup>14</sup>
  - Private foundation.<sup>15</sup>

## 2.2 Role of trust and corporate services providers

Many countries, territories and jurisdictions qualify as OFCs and include well-known centres like Switzerland, Bermuda and the Cayman Islands, and lesser-known centres like Mauritius, Dublin and Belize. The level of regulatory standards and transparency differs widely among OFCs.

Greater emphasis is placed on offshore jurisdictions in the context of criminal investigations because some offshore jurisdictions provide excessive secrecy for their corporate vehicles and create a favourable environment for their use for illicit purposes. Shell companies constitute a substantial proportion of the corporate vehicles established in some OFCs. Given their function, shell companies face an increased risk of being misused. Furthermore, a number of other offshore jurisdictions have developed specialised, sophisticated and robust regimes for obtaining and sharing information on beneficial ownership and control and/or are undertaking serious efforts to strengthen their regulatory, supervisory and legal regimes in order to curtail the use of corporate vehicles for illicit purposes.<sup>11</sup>

The bedrock of most OFCs is the formation of offshore structures, typically inclusive of the following:

In many instances, corporate vehicles or offshore structures, such as shell companies or trusts,<sup>16</sup> are misused to conceal or disguise the criminal’s beneficial ownership of illicit proceeds. Banking institutions act as obvious gatekeepers for the legitimate financial system facilitating ‘access’ to the world of such structures and the financial system. However, persons and/or entities other than banking institutions, such as TCSPs, trust companies, legal professionals, accountants and financial advisors, in many ways have moved to ‘centre stage’ in the fight against money laundering, both globally and locally. Criminal organisations and individuals use TCSPs to assist with illicit activities by seeking professional services and advice on the most appropriate vehicles or jurisdictions to use to further their ill-intended agendas. Due to their knowledge and expertise, TCSPs are well-placed to facilitate money laundering and the concealment of assets generally. Not only can they facilitate the commission of the predicate

12 The term offshore company is ambiguous. It may refer to either:

1. A company which is incorporated outside the jurisdiction of its primary operations regardless of whether that jurisdiction is an OFC (sometimes known as a non-resident company); or

2. Any company (resident or otherwise) incorporated in an OFC, i.e. offshore jurisdiction.

13 An offshore trust is simply a conventional trust that is formed under the laws of an offshore jurisdiction.

14 An offshore partnership is, in essence, a legal contract entered into by two or more persons, in terms of which each agrees to furnish a part of the capital and labour for a business enterprise, and by which each shares a fixed proportion of profits and losses.

15 A private foundation is a legal entity set up by an individual, a family or a group of individuals for a purpose, such as philanthropy or an object legal in the economic operation. The Bill & Melinda Gates Foundation is the largest private foundation in the United States of America (USA).

16 Described in greater detail in paragraph 4.3 below.

11 2001 OECD Report, op. cit., p.7.

offence and layering of criminal property, but they can also assist the beneficial owners of criminal assets in disguising or concealing their ownership of such property.

TCSPs are often involved in designing corporate vehicles as they offer a wide range of services, including company incorporation, director services, nominee shareholder services, company secretarial services, registered office services and trustee services. TCSPs have a unique insight into the daily operations and real 'financial life' of corporate vehicles and can be an invaluable source of information to the practitioner if he knows who to approach and what to request.

TCSPs are very often owned by private banks and service the clients of those banks. Frequently, TCSPs offer 'trust and company packages' inclusive of registered office, directors, shareholders and book-keeping services for as little as GBP 2,500. Employees of these companies sign 'legitimate' contracts on behalf of the companies (which, in turn, are often owned by trusts) they purport to 'manage and control' for very large sums of money and for little reward. These TCSPs also act as trustees for the trusts, which own the company through nominee shareholders provided by the TCSPs.

### 3. Beneficial ownership

During a criminal investigation involving corporate vehicles, particularly those formed in offshore jurisdictions, the crux of the issue for any practitioner is unravelling the 'beneficial owner' of the corporate vehicle.

Beneficial owner refers to the natural person(s) who ultimately owns or controls an asset and directly or indirectly enjoys the benefit thereof. He/she also owns or controls the customer and/or the natural person, who may appear to own or control the asset, on whose behalf a transaction is being conducted in order to hide the true ownership. It also includes those persons who exercise ultimate effective control over a legal person or arrangement. 'Ultimately owns

or controls' and 'ultimate effective control' refer to situations in which ownership/control is exercised through a chain of ownership or by means of control other than direct control.

In contrast with the 'beneficial owner', the legal or nominee company owners and trustees might be registered as the legal owners of an asset without actually possessing the right to enjoy its benefits. Complex and opaque corporate structures set up across different jurisdictions make it easy to hide beneficial owners, especially when use is made of nominees in their place and part of the corporate structure is incorporated in a jurisdiction known for its secrecy.

As stated above, it is essential to be able to 'see through' the corporate veil provided by the structure to identify the controlling party, i.e. the beneficial owner.<sup>17</sup> The most important question is: **who is in control?** Understanding who is in control of a corporate vehicle is essential for investigative purposes in order to identify the true person(s) behind it. Legal and beneficial ownership information can assist law enforcement and other competent authorities by identifying those natural persons who may be responsible for the underlying criminal activity. It also assists in identifying those who may have information of relevance to the investigation, and thus it further assists in 'following the money' in financial investigations involving suspect accounts/assets held by corporate vehicles.

### 4. Typical corporate vehicles used for criminal purposes

Experience dictates that corporate vehicles play a central role

<sup>17</sup> The purpose of the FATF standards on transparency and beneficial ownership contained in Recommendations 24 and 25 is to prevent the misuse of corporate vehicles for money laundering and terrorist financing. However, in recognition of the challenges posed with regard to implementation, FATF recently developed a guidance paper to assist countries - 'Transparency and Beneficial Ownership', October 2014, viewed on 20 November 2014. Available at <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-transparency-beneficial-ownership.pdf>.

in concealing the abuse of public trust for private financial gain, money laundering and the beneficial ownership of illicit assets. During recent research<sup>18</sup> into the corporate and financial structures that form the building blocks of hidden money trails, the World Bank/United Nations Office for Drugs and Crime (UNODC) Stolen Asset Recovery Initiative (StAR) focused on the ease with which corrupt actors hide their interests behind a corporate veil. The research also covered the difficulties investigators face in trying to lift that veil. The majority of cases share a number of common characteristics, including:<sup>19</sup>

- A corporate vehicle was misused to hide the money trail;
- The corporate vehicle in question was a company or corporation;
- The proceeds and instruments of corruption consisted of funds in a bank account; and
- In cases where the ownership information was available, the corporate vehicle in question was established or managed by a professional intermediary.

In the vast majority of analysed grand corruption cases, corporate vehicles, including companies, trusts, foundations and fictitious entities, were misused to conceal the identities of the people involved in the corruption. Of these corporate vehicles, the company was the most frequently used.

Corrupt public officials and money launderers do not want to keep their dirty money in their own names. Therefore, what they typically do is create a company - or a series of

companies - and have the company own their assets. The company can open a bank account, it can buy a yacht or a mansion, and it can wire money around the world. Most importantly, it is immensely difficult and sometimes totally impossible to link the company back to the person who really owns it. This makes it an attractive mechanism for hiding, moving and using money or other assets.<sup>20</sup>

While major corruption cases often have an international dimension, practitioners have very little knowledge of corporate vehicles outside their own country and often lack the resources to obtain evidence from other jurisdictions.

Rather than attempt to cover each and every type of corporate vehicle, this chapter will focus on the most commonly used structures.

#### 4.1 Shell companies

A shell company can be defined as a non-operational company, i.e. a legal entity that has no independent operations, significant assets, ongoing business activities or employees.<sup>21</sup> In its most typical form, a shell company is provided by a professional intermediary to a corrupt party who then uses it to obscure the money trail as the illicit funds in question are transferred into and through bank accounts.

Shell companies can be formed to serve a variety of legitimate economic functions, such as facilitating a merger, sequestering liabilities or holding stock or intangible assets of another business entity. However, they can also be misused

18 'Puppet Masters: How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do About It', 2011, The International Bank for Reconstruction and Development/The World Bank. Available at <http://star.worldbank.org/star/sites/star/files/puppetmastersv1.pdf>. This report provides an invaluable resource for practitioners when investigating how corporate vehicles, like companies, trusts and foundations, facilitate major corruption.

19 Puppet Masters, op. cit., p.2, para. 1.

20 Puppet Masters, op. cit., p. 33, para. 3.1.

21 Although the FATF Recommendations make no use of the term 'shell company' per se, the 2001 OECD Report defines them at p. 17 as 'Companies, which are entities established not to pursue any legitimate business activity but solely to obscure the identity of their beneficial owners and controllers, constitute a substantial proportion of the corporate vehicles established in some OFCs [off shore financial centers]'.

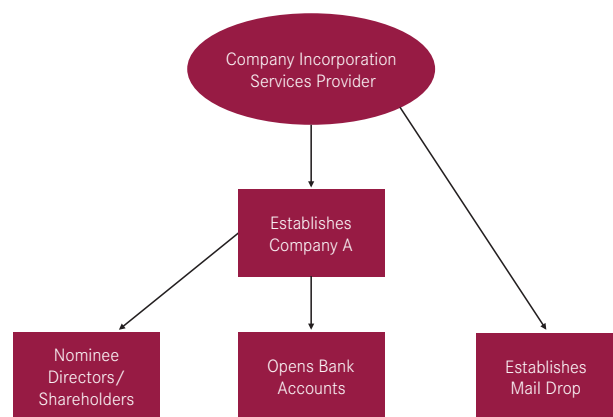
by illicit actors and have no legitimate commercial purpose.<sup>22</sup> To facilitate money laundering operations and other illicit schemes, shell companies may be used to generate false invoices, fictitious consultancy fees or commission payments, or bogus loans.

A shell company has no physical presence in its jurisdiction. It is usually formed in a tax haven or secrecy jurisdiction, and its main or sole purpose is to insulate the real beneficiary (beneficial owner) from taxes, disclosure or both. Shell companies are also referred to as front companies or 'mailbox/letterbox' companies. One specific type of shell company structure is the international business corporation (IBC), which is typically used for shell companies set up by non-residents in OFCs. By definition, IBCs make ideal shell companies because they are not permitted to conduct business within the incorporating jurisdiction and are generally exempt from local income taxes.

It is quick, easy and cheap to set up an anonymous shell company. Shell companies commonly used to give and receive bribes, launder money and evade taxes are also easily available online for a few hundred dollars.

'A company-formation agent's fees range from USD 800 to USD 6,000 as an upfront cost, followed by a slightly smaller amount on an annual basis. Costs may vary, depending on whether the service provider provides additional services, such as nominee director or shareholder arrangements, filing of any annual documentation, or phone and mail forwarding'.<sup>23</sup>

Box 1 – Basic shell company structure



Shell companies, often together with other tools used in financial crimes, can be established to disguise the trail of the evidence by establishing layers between the criminal and the laundering, fraudulent or corrupt transaction, and between the predicate crime and the criminal proceeds.

Consider the following example: In return for highly lucrative mining contracts with Country A, Company X paid large bribes to those awarding the contracts. Yet a direct transfer from the company to the officials in question would be extremely suspicious, even to a government intent on looking the other way. So, instead, Company X used a middle-man insulated from the company and the ultimate recipient by two shell companies with nominee directors and shareholders – one between the middleman and Company X and the other between the middleman and the recipient. The financial flows between each link in the chain are dressed up as payments for vague 'consultancy' and 'marketing' services. To prove that a corrupt agreement has been struck, investigating authorities face the very difficult task of following each link in the chain across different jurisdictions to prove that these ostensibly independent parties are, in fact, all part of the same criminal enterprise.

Shell companies, when used illicitly, are generally used in combination with additional mechanisms to obscure

22 FATF, 'Money Laundering Using Trust and Company Service Providers', October 2010, p.34, para. 104.

23 Puppet Masters, op. cit., p. 35, Box 3.1.

beneficial ownership. Other mechanisms include exercising control surreptitiously through contracts (rather than 'standard' ownership and control positions), adding layers of corporate vehicles, hiding behind bearer shares<sup>24</sup> and ensuring that the beneficial owners are located (or the identifying information is stored) in another jurisdiction.<sup>25</sup>

As shell companies, unlike normal companies, have no economic activity, it is difficult to find out much information about them. A normal company that is engaged in business will typically market itself, join a chamber of commerce, build a website, sponsor charitable events and buy supplies and equipment. It will have employees who can be interrogated, keep meeting minutes that may be consulted and produce financial data that can be compared with normative industry benchmarks. A non-operational company, like a shell company, may do some of these things (companies are often obligated to hold a meeting of shareholders once a year) but probably does not have to.

However, it is useful to remember that shell companies do not exist, and therefore incorporators of such companies face difficulties in faking an active and robust online presence. Such a presence would include the existence of a well-designed website, the presence of other online content, periodic and regular updates of information, and contact email addresses that are linked to a legitimate website address, not free email accounts. If the company has no online presence at all and no available online information to be expected of a company engaged in such a business, the investigator begins to uncover information that may lead to the unravelling of an entire shell network.

Criminals often make use of a network of shell companies to conceal beneficial ownership of illicit assets or a money laundering scheme, making the identification and investigation of such companies time-consuming and difficult without resources and assistance. Therefore, practitioners should take full advantage of online resources, particularly online organisations that are involved in various aspects of investigating, reporting and/or tracking shell companies and criminal investigations.<sup>26</sup>

## 4.2 Shelf companies

Shelf companies are a category of, and are similar to, shell companies in that they offer no real 'brick and mortar' company.

A shelf company is a corporation that has had no activity. It has been created, left dormant and put on the 'shelf'. This corporation is then later usually sold to someone who would prefer to have an existing corporation than a new one.<sup>27</sup> The significant difference between shell and shelf companies lies in the age of the respective companies since incorporation, with the value of a shelf company being based upon its history and banking relationships in addition to its age.

A shelf company is a company that has already been incorporated with a standard memorandum and articles of association and has inactive shareholders and directors

24 According to the FATF Misuse Report, op. cit. Annex 1 Glossary, p. 23, they are defined as 'negotiable instruments that accord ownership of a corporation to the person who possesses the bearer share certificate'. Bearer shares are negotiable instruments that can be easily transferred without leaving a paper trail. Although they can serve legitimate purposes, they can also be used to mask the true ownership and control of a company and thus may be used for money laundering, self-dealing and/or insider trading.

25 Puppet Masters, op. cit., p. 35.

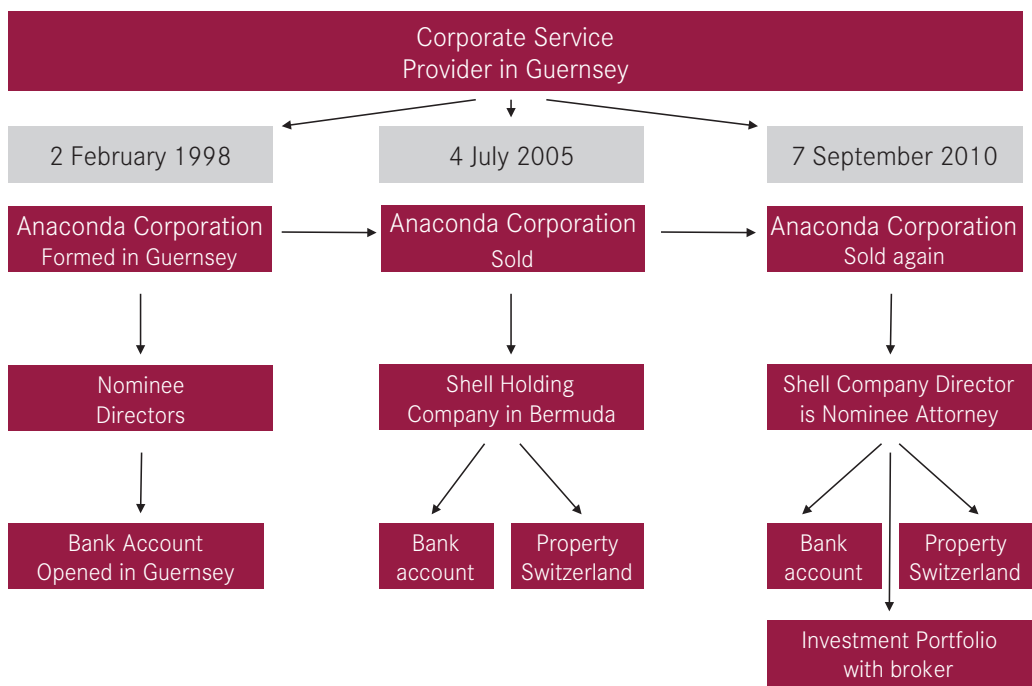
26 These include the following:

- FATF, available at [www.fatf-gafi.org](http://www.fatf-gafi.org);
- The Puppet Masters, op. cit.;
- Global Witness, available at [www.globalwitness.org](http://www.globalwitness.org);
- Office of Foreign Assets Control (OFAC), available at [www.treasury.gov](http://www.treasury.gov);
- Financial Crimes Enforcement Network (FinCen), available at [www.fincen.gov](http://www.fincen.gov);
- Offshore Alert, available at [www.offshorealert.com](http://www.offshorealert.com); and
- International Consortium of Investigative Journalists (ICIJ), available at [www.icij.org](http://www.icij.org).

27 FATF Misuse Report, op. cit., p. 24.

as well as an inactive secretary. When a shelf company subsequently is sold, the inactive shareholders transfer their shares to the purchaser, and the directors and secretary submit their resignations. Typically, the authorities do not need to be notified when a shelf company is sold.

Box 2 – Use of shelf companies



An advertisement for a shelf company typically emphasises the benefits inherent in shelf corporations and aged corporations, which establish immediate corporate history. For example, Companies Incorporated<sup>28</sup> holds a list of ‘pre-filed’, off-the-shelf companies that one can acquire. By owning a pre-established corporate entity, one is able to take advantage of instant availability and fast delivery, and one can show longevity of company filing and immediately own a company with a filing history. It is ready for immediate

transfer as no stock are currently issued and may help when applying for contracts and financing. It is also easier to obtain business credit cards and business credit lines.

In some jurisdictions, incorporation procedures can be time-consuming so it is often easier, quicker and less expensive to transfer ownership of a shelf company than it is to incorporate a new one. Lenders sometimes require a business to have been in existence from six months to two years or more before lending it money. Many agencies will only sign contracts with a company that has been in business for at least two years.

28 Available at <http://www.companiesinc.com/corporation/aged> and <http://www.unitrustcapital.com/services.html>.

The price of an 'aged' shelf company available for immediate purchase tends to vary depending on how long it has existed. For example, for a company less than five years old, one might expect to pay USD 1,000 per year that the company has existed. In the case of a company more than 10 years old, this sum might increase to USD 35,000. Costs increase in cases in which the shelf company offers additional benefits, such as pre-existing lines of credit, maintained records and bank accounts.

Shelf companies are a concern to law enforcement authorities, because criminals can easily throw investigators off the trail by purchasing shelf companies and then never officially transferring the ownership, i.e. registering with the authorities. In such cases, the investigation often leads to a dead-end formation agent who has long ago sold the company with no records of the purchaser and no obligation to note the ownership change.

### 4.3 Trusts

The concept of a trust is probably less familiar to most than that of a company, but it has been around for a considerably longer period of time. The trust is a legal relationship that originated historically in England, and consequently, developed mainly in states with a Common Law or Anglo Saxon legal tradition, e.g. Great Britain, the USA, Australia, Canada, South Africa and New Zealand. In addition, institutions similar to trusts can be found in other countries, e.g. Japan, Panama, Liechtenstein, Mexico, Colombia, Israel and Argentina.<sup>29</sup>

<sup>29</sup> It should also be noted that some countries, such as those in the Middle East and North Africa (MENA) region, recognise a type of trust called a Waqf, an inalienable religious endowment in Islamic law. It refers to a voluntary and irrevocable dedication of one's wealth or a portion thereof - typically a building or plot of land or even cash - for Muslim religious or charitable purposes where the donated assets are held by a charitable trust. However, although similar, the Waqf would appear to differ in one essential respect, i.e. it relies on a contractual basis for its establishment, whereas the trust (as it is understood in the United Kingdom [UK] and many other countries with a Common Law or Anglo Saxon legal tradition) is a legal relationship or arrangement between various parties and not a mere contract (to be described in greater detail later).

A trust is a legal arrangement or relationship that exists in many jurisdictions when a person ('trustee') owns assets, not for one's own use and benefit, but for the benefit of others ('beneficiaries'). Unlike companies or corporations, it is a corporate vehicle that does not have a separate legal personality and distinguishes legal ownership from beneficial ownership. It constitutes a binding obligation in terms of which the ownership of assets is transferred to a trustee(s) by means of a trust deed,<sup>30</sup> which are to be managed and used for the benefit of named or unnamed beneficiaries.

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. Consequently, the idea of split ownership of property emerged, whereby the crusader (or those nominated by him) was treated as having a beneficial interest in the land and the person left in charge as the legal owner of the land. The basic concepts still hold true today.

Trust relationships are formed for many reasons and purposes, and it is impossible to set out an exhaustive list of the types of trusts. A trust may be tailored to achieve any purpose as long as it is not against public policy, illegal or in contravention of certain fundamental tenets of trust law. The terms of the trust identify the law applicable to it. Furthermore, through the adoption of the Hague Convention on the Law Applicable to Trusts and their Recognition (1985), member countries recognise the existence and validity of trusts but, inter alia, only those which are created voluntarily and evidenced in writing. Within limits, the purpose for which trusts may be used is restricted only by the imagination of the various parties concerned as well as their professional advisers.

In practice the trust has proved to be an extremely flexible

<sup>30</sup> To be described in greater detail later.



instrument and can be used for many legitimate and commendable purposes. It is frequently used in connection with estate planning and for so-called asset protection for individuals. The problems arise when the trust is used to conceal the origin and distribution of illegal funds. Unfortunately, trusts that hide the identity of the parties to the trust have become a standard part of money laundering arrangements.

The essential components or parties to a trust are the settlor, the trustee, the beneficiaries and the trust property. The settlor transfers ownership of his assets to trustees by means of a trust deed,<sup>31</sup> which are to be managed and used for the benefit of named or unnamed beneficiaries. This constitutes a binding obligation. In the process of transferring (or 'settling') certain property, the legal ownership or control of the assets (known as the trust property) is separated from the beneficial interest in such assets.

The express trust is the most common trust and includes both fixed and discretionary trusts. With a discretionary trust, the interests of the beneficiaries are not fixed but depend upon the exercise by the trustee of some discretionary powers in their favour. As such, it is the most flexible of all trusts and often used by criminals, because the beneficiary can be named or changed at any time, making it possible to keep the beneficiary's identity secret up until the time the ownership of the assets held in trust is transferred to him.

Where the trustee has some discretion as to the investment and distribution of the trust's assets, the deed may be accompanied by a non-legally binding letter, known as a Letter of Wishes. A Letter of Wishes, which often accompanies discretionary trusts, sets out the settlor's wishes regarding how he desires the trustee to carry out his duties, from whom the trustee should accept instructions and who the beneficiaries should be (which may include the

settlor himself). While a Letter of Wishes is not legally binding on the trustee, he usually follows the wishes expressed in the Letter of Wishes.<sup>32</sup>

As stated above, the trust does not have a separate legal personality, and the trustee holds the trust assets on a fiduciary basis. However, on the other hand, the trust is not just a mere contract. Although the trust is originally set up by the settlor, after its creation it is essentially a legal relationship or arrangement between juridical persons – settlor, trustee and beneficiary<sup>33</sup> – which is principally governed by the trust agreement or trust deed and secondarily by the specific rules of the applicable legal system.

A beneficiary is a person who is designated to receive something as a result of a trust arrangement. While trusts must always have some ultimately ascertainable beneficiary, trusts may have no defined existing beneficiaries but only objects of a power until some person becomes entitled as beneficiary to income or capital on the expiry of a defined period, known as the accumulation period. This period is normally co-extensive with the trust's perpetuity period, which is usually referred to in the trust deed as the trust period.<sup>34</sup>

'A trustee, who may be a paid professional or company or unpaid person, holds the assets in trust fund separate from their own assets. The trustee invests and disposes of the trust assets in accordance with the settlor's trust deed, taking account any letter of wishes. There may also be a protector, who may have power to veto the trustee's proposals or remove them, and/or a custodian trustee, who holds the assets to the order of the managing trustees'.<sup>35</sup>

On the creation of a trust, there must be a transfer of ownership of money or property; however, there is no

31 Reference is also sometimes had to a declaration of trust as a form of trust instrument. It differs from the trust deed, in essence, insofar as it does not have to mention, or be signed by, the settlor with the trustee being the only named party, thus carrying a high degree of confidentiality.

32 2001 OECD Report, op. cit., p. 26, para. 2.

33 FATF Misuse Report, op. cit., Annex 2 Explanatory Note: Trust, p. 25, pt. 5.

34 FATF Misuse Report, op. cit., Annex 1 Glossary, p. 23.

35 2006 FATF Report, op. cit., Annex 1 Glossary, p. 24.

minimum amount of capital that must be transferred from the settlor to the trustee. 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. As stated above, in some jurisdictions a 'declaration of trust' obviates the need for a settlor to be named at all during the establishment of the trust.

In setting up the trust, the settlor has comparatively extensive freedom. However, once the trust is established, he only has a limited degree of influence over the trust. After the trust is created, the trustee's primary duty is to safeguard the interests of the beneficiaries and not those of the settlor.

It is normal, but not essential, for a trust to be constituted in writing in the form of a 'trust deed' or trust instrument, which will set out the following:

- The manner in which beneficiaries can benefit from the trust; and
- The powers/duties that trustees will have in administering the trust and its assets.

Trusts are not required to register in many jurisdictions, which can therefore pose difficulties in identifying the

beneficial owner of a trust.<sup>36</sup>

The separation of the legal ownership of the trust assets (which lies with the trustee) from the right to benefit from those assets (which lies with the beneficiaries) is the crucial factor to an understanding of trusts. Very often confusion is created, because the person (the 'settlor') who transfers assets to the trustee does not appreciate that in so doing he loses all title and control over those assets, including control over how they are managed, unless he reserves specific powers in the trust deed. If the intended purpose of the trust can be attacked by revealing that the settlor (the criminal) still controls the assets, this poses a major breakthrough in any investigation.

In many instances, the trustee's duty of confidentiality is used as justification for resisting the disclosure of trust information. However, this issue was recently discussed and, to some extent, clarified in the Guernsey Court of Appeal decision of *In re B; B v T* (Court of Appeal, 11 July 2012). In an analysis of when disclosure would be appropriate, the duty of confidentiality owed by a trustee to a beneficiary was described as akin to that owed by a bank to a customer.

36 It should be borne in mind that the final text of the Fourth European Money Laundering Directive (and the draft adopted by the European Parliament in March 2014) provides for the establishment of a registry for trusts. For the first time, European Union (EU) member states will be obliged to maintain central registers listing information on the ultimate beneficial owners of corporate and other legal entities as well as trusts. These public registries are, however, not fully public, but 'Any person or organisation who can demonstrate a "legitimate interest", such as investigative journalists and other concerned citizens, would also be able to access beneficial ownership information such as the beneficial owner's name, month and year of birth, nationality, residency and details on ownership.' The deal still needs to be endorsed by EU member states' ambassadors (COREPER) and by Parliament's Economic and Monetary Affairs and Civil Liberties, Justice and Home Affairs committees before being put to a vote by the full Parliament in 2015.

Available at <http://www.step.org/european-ministers-debate-amend-money-laundering-directive-next-week> and <http://www.europarl.europa.eu/news/en/news-room/content/20141216IPR02043/html/Money-laundering-Parliament-and-Council-negotiators-agree-on-central-registers>.

Citing the well-known English case of *Tournier v National Provincial and Union Bank of England* [1924] 1 K.B. 461, the court held that trustees have a general duty of confidentiality but that such duty was not absolute and could be qualified, inter alia, where disclosure is under compulsion by law. Ultimately, there are limits to the duty of confidentiality, particularly in light of potential injustice, and a criminal investigation into money laundering or corruption would justify disclosure.

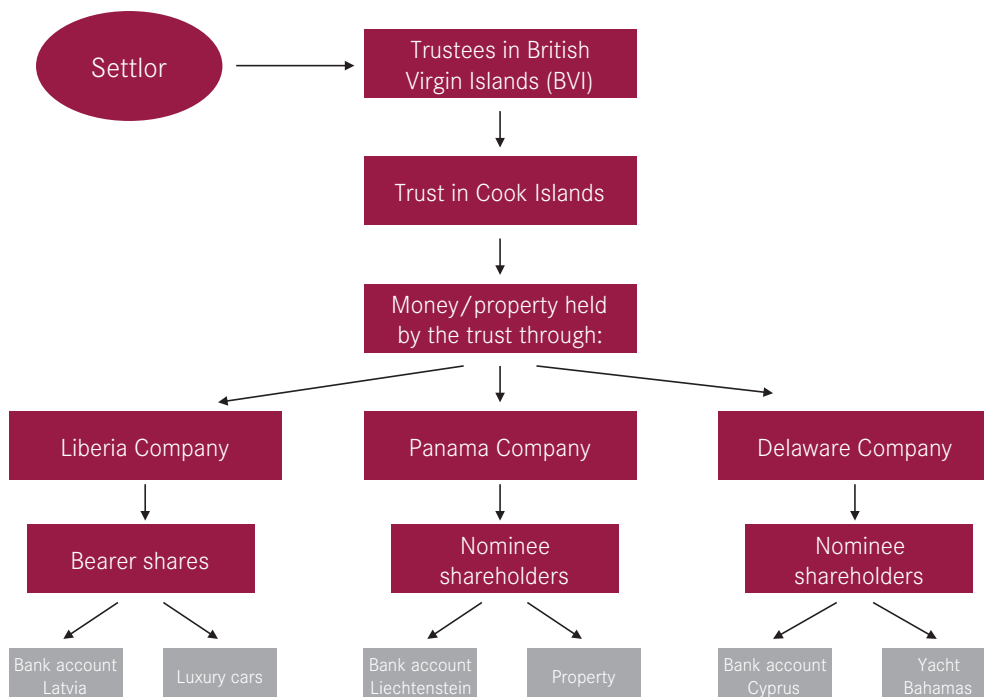
A simple trust structure utilised for criminal purposes would entail the following:

The settlor uses trustees in the British Virgin Islands, e.g. a trust company providing trust services, to establish a discretionary trust in the Cook Islands, 'settling' a nominal amount of money in the trust. The trust subsequently acquires various assets with the proceeds of crime through the following:

A simple trust structure utilised for criminal purposes would entail the following:

- A company, incorporated in Liberia and owned through bearer shares, with a bank account in Latvia and luxury cars;

Box 3 – Trust structure for criminal purposes



- A company, incorporated in Panama with nominee shareholders holding shares on behalf of the trust, with a bank account in Liechtenstein and property elsewhere; and
- A company, incorporated in Delaware with nominee shareholders holding shares on behalf of the trust, with a bank account in Cyprus and a yacht in the Bahamas.

Further investigation will reveal that the trust has discretionary beneficiaries so, in effect, the assets are owned via bearer shares and nominee shareholders by companies in which the beneficiary has a discretionary interest. To prove that the settlor (the suspect) is actually the beneficial owner, the evidence must show he controls the trust for his own benefit by 'dictating' to the trustee how he should exercise his discretion.

## 5. Establishing control and benefit

A key challenge in the investigation of corporate vehicles is to unravel beneficial ownership by proving who is in control. The criminal's main desire is to be able to benefit from his ill-gotten gains, sometimes at great risk of alerting the criminal authorities and making mistakes, and one piece of information can very often begin the process of piercing the veil. There are various investigative techniques available for use in this process, including databases (such as the website established by the ICIJ mentioned above<sup>37</sup> that leaked records of names behind covert companies and private trusts), but no single formula other than the practitioner

being as creative as the criminal himself.

Not only must the practitioner determine who controls the corporate vehicle but he must also establish who ultimately benefited from the structure. As with the investigation of any proceeds-generating crime, this involves conducting a financial investigation to identify and document the movement of funds, i.e. following the money trail. The link between the origins of the money, recipients, when the money was received and where it is stored or deposited can provide information to identify the beneficiary.<sup>38</sup>

The financial sector can prove a very valuable source of information for the practitioner engaged in a financial investigation and asset tracing. The good practitioner knows the nature of requirements that are placed on financial institutions arising from the anti-money laundering framework (AML), in particular with regard to customer due diligence (CDD) and record keeping requirements.<sup>39</sup> This knowledge allows him to ask the right questions and request relevant documentation, such as background reports on the individual business relationship in addition to correspondence, risk assessments, bank account records, account opening documents, etc.

The due diligence requirements<sup>40</sup> imposed on financial institutions include, for example, the identification of the beneficial owner (in addition to the customer) and taking reasonable steps to verify the identity of the beneficial owner to the extent that the financial institution is satisfied that it knows who the beneficial owner is. This should include financial institutions taking reasonable measures to understand the ownership and control structure of the customer where legal persons and arrangements are concerned. Special attention should be paid to financial products that raise suspicion by their very nature, such as when the customer does not coincide with the beneficial

37 ICIJ is a global network of 185 investigative journalists in more than 65 countries who collaborate on in-depth investigative stories. It was launched as a project of the Centre for Public Integrity to extend the Centre's style of watchdog journalism, focusing on issues that do not stop at national frontiers. ICIJ reporters and editors provide real-time resources and state-of-the-art tools and techniques to journalists around the world. Available at <http://www.icij.org/offshore/secret-files-expose-offshores-global-impact>.

38 See chapter 3 on financial profiling.

39 See chapter 5 on money laundering and asset tracing, at paragraph 4 dealing with 'The use of AML preventive measures in asset tracing'.

40 FATF Recommendation 5.

owner (joint accounts, joint securities accounts, investment companies and other collective investments), offshore companies, customers 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).

If corporate vehicles have been formed to hide the true ownership of the funds, the financial tracing will often penetrate the web of confusion by identifying the beneficial owner of the money. The person enjoying the fruits of the crime - that is, the person driving expensive cars and living in luxury vacation properties - is the beneficial owner.

### 5.1 International cooperation

Where criminal assets are registered to offshore structures, international cooperation should facilitate the provision of investigative assistance in obtaining documents and evidence to unravel beneficial ownership (to the extent possible). Knowing how to approach an investigation with a transnational component, making use of multi-lateral and bilateral treaties, letters of request and informal channels is a vital tool in the toolkit of any practitioner tasked with connecting criminal proceeds to the criminal.<sup>41</sup> It is also important to know what is available in different jurisdictions and how to obtain such information as cooperative efforts between jurisdictions are essential to the successful conclusion of the investigation.

The investigative process in such cases is based on the use, analysis and cross-checking of a myriad of sources, both documentary and human, in the relevant jurisdictions. These must take into account business and legislative environments that vary from country to country and sector to sector. The more sophisticated the offshore structure, the more complex the investigation. One of the key elements of research and analysis is to look for inconsistencies and mistakes.

The success of an investigation often depends largely on

---

41 See chapter 4 on mutual legal assistance.

the practitioner's ability to utilise all the powers, tools and sources available to him to gather evidence and trace assets. A particular source of intelligence that has become increasingly utilised in the past decade is open source intelligence, which involves the acquisition and analysis of information from publicly available sources.<sup>42</sup> Examples of such sources include publicly available databases (such as property and corporate databases) that can be easily located using publicly available search engines, such as Google, or analysed using specifically tailored programmes, such as the International Centre for Asset Recovery (ICAR) Asset Recovery Intelligence System (ARIS) tool.

Searches should not only target the trust or company but also associated entities and possible links. All the individuals involved, including nominees, fiduciaries and other third parties involved in offshore structures, should be profiled. The most important task is to map every piece of information uncovered locally and abroad and to document the links no matter how small or insignificant each individual piece may appear. An address or telephone number could provide the key to uncovering the shell network. In order to ensure no single piece of information is overlooked, practitioners should make use of mapping and relationship tools, such as the free online tool yEd.<sup>43</sup> The information should then be matched with the details provided by the suspect in order to identify any inconsistencies and peculiarities. An example of an inconsistency might be when a beneficial owner (suspect) declares he has no assets. Investigation establishes that a nominee, who is listed as director of a number of corporate vehicles associated with the suspect, manages assets worth millions. It is possible that the suspect owns these assets. It must be established that assets are disbursed for his benefit and at his 'request'.

---

42 See chapter 2 on case strategy and investigation.

43 yEd is a powerful desktop application that can be used to quickly and effectively generate high-quality diagrams. It can be downloaded free of charge and used to draw many different types of diagrams, including flowcharts, network diagrams, organisation charts and Entity Relationship diagrams, or import one's external data for analysis. Available at [http://www.yworks.com/en/products\\_yed\\_about.html](http://www.yworks.com/en/products_yed_about.html).

## 5.2 Relevant documentation/information

It is necessary to focus on and obtain all possible information from the TCSPs. As a general rule, the providers of trusts, for example, rather than the trusts themselves are increasingly the subject of regulation, as trusts constitute private arrangements and a legal relationship and do not amount to artificial entities as in the case of companies which are separate legal personae. Therefore, in order to 'see through'

the corporate veil provided by a structure to identify the controlling party, the practitioner is more likely to obtain relevant information/evidence from the TCSPs or other professionals responsible for establishing/managing the structure.

The following table provides an example of the type of information that can be sourced in respect of trusts and companies:

### TRUST

- Full details of settlor and trustee;
- Trust deed, variations thereof;
- Trustee minutes and resolutions;
- Letters of Wishes;
- Any correspondence, powers of attorney, emails and instructions;
- Beneficiary details and letters of addition or removal of beneficiaries;
- Accounts (which have to be kept) of trusts although these would not be audited;
- Schedules of assets;
- Correspondence with all investment managers;
- Regular valuations;
- Decisions taken by trustee, e.g. appointments of capital, distributions of income, references to changes or variations of the trust instrument, any significant changes or transactions involving trust assets; and
- File notes/telephonic transcripts. (It is common practice for the trustee to receive a phone call from a settlor with a discretionary interest in a trust asking for a distribution or a loan to be made. Failure to note and treat it as a request but rather as an instruction may lead to the conclusion that the settlor is controlling the trust assets.)

### COMPANY

- Articles of Incorporation;
- Shareholding;
- Statutory books;
- Authorised and issued share capital/copies of share certificates and bearer shares; and
- Any correspondence, powers of attorney, emails or instructions.

If a trust has not been properly constituted, this may well assist the investigator in identifying/confirming the actual beneficial owner of the structure. For example, if the settlor (suspect) purports to have established a trust and yet maintains control of the trust property, it will not be upheld as a trust. By showing that he gives instructions to the trustee regarding disbursements from the trust bank account and furthermore benefits in the process, this will assist in dispelling the notion of a trust and confirming beneficial ownership of criminal proceeds.

It is also important to obtain a complete set of financial records from the banks involved as this will assist in the financial portion of the investigation. All memoranda, correspondence or emails associated with the accounts should also be obtained, and all cheques, wire transfers, debit/credit memoranda and account activity should be carefully reviewed and analysed.

In respect of property purchases, a complete set of closing/settlement records, including all notes, file memoranda and emails, and all back-up documents for mortgage payments should be obtained. The identity of any individuals receiving and sending mail at the property should be determined in addition to records of the source of funds paid to conveyancers or attorney trust accounts.





# 7. Tracing digital currencies

Federico Paesano

- 1. Understanding digital currencies **115**
  - 1.1 General characteristics **115**
  - 1.2 Where are one's bitcoins? **116**
  - 1.3 Legislative characteristics **117**
- 2. Tracing digital currencies **118**
  - 2.1 Digital currencies and criminals **118**
  - 2.2 The blockchain as an investigative tool **119**
  - 2.3 Investigative techniques **119**
  - 2.4 Case study: Silk Road **122**
- 3. Final considerations **124**



## 1. Understanding digital currencies

In recent years, financial payments have experienced an unprecedented wave of technological innovations with the development of new electronic payment methods. These instruments increase concerns over money laundering and terrorist financing as the new technologically advanced channels can also be used for criminal purposes. Technology moves extremely fast while legislators are usually slow to adapt. The difference in the pace between the two sides eventually creates a gap that is readily exploited by criminals. This is particularly true when it comes to new ways of moving money around the globe. Financial transactions, which have always involved cash or cash-derived instruments, now can be completed with new technologies, like the Internet, mobile payments and card instruments, rapidly gaining acceptance worldwide. They will (and already have had) an impact on the effectiveness of existing investigative techniques and best practice for financial crimes. These *modi operandi* were based on past experience, such as the use of cash, cheques and bank accounts to conduct transactions, and relied heavily on the mandatory obligation for financial institutions to apply thorough know your customer (KYC) requirements. The new payment methods that have been developed recently can render previous techniques and best practice obsolete and challenge the way in which financial investigations are conducted.

Digital currencies have the potential to make it easier for criminals to hide the source of their proceeds and move their funds across borders without detection. Recent cases (such as Liberty Reserve and Silk Road) show that criminal organisations are already using digital currencies to launder their proceeds of crime. On the other hand, these cases have also shown that, although difficult, the investigation of the ownership of digital currencies is not impossible. Digital currency networks usually record transactions in a distributed public ledger (to be described in greater detail below), which can be subjected to analytical monitoring tools capable of highlighting suspect transactions. A digital transaction always leaves a trace. Once the veil of secrecy

is pierced assets can be sought, found and confiscated.

### 1.1 General characteristics

Digital currency is usually defined as a currency or medium of exchange that is electronically created and stored (i.e. distinct from physical media, such as banknotes and coins). As such, this definition applies to virtually every currency in existence today (USD, EUR, etc.). Some of them (like bitcoin) are 'cryptocurrencies', a type of digital token that relies on cryptography (for chaining together digital signatures of token transfers), peer-to-peer networking and decentralisation. Cryptocurrencies, due to their characteristics, are currencies that pose greater concerns when involved in a financial investigation. This chapter will focus on cryptocurrencies and particularly on bitcoin,<sup>1</sup> which almost all the other cryptocurrencies are based upon.

#### DIGITAL AND CRYPTO CURRENCY

A vast majority of the money supply in the world (USD, EUR, GBR, etc.) is created and traded exclusively in a digital form held and managed on computers. In a society that is becoming more cashless everyday, all our currencies are becoming digital currencies, although their creation is still managed by central banks with their expansionary monetary policies. *Cryptocurrencies* are not influenced by any government. Their creation is decentralised and relies exclusively on a pre-determined mathematical process that limits the quantity of new currency created.

A certain level of privacy, the speed of transactions and the very low cost involved are among the characteristics that fuel the increasing adoption of cryptocurrency. Its community is growing daily, attracting an increasing number of users,

<sup>1</sup> The word 'Bitcoin' (with a capital 'B') is used when referring to the concept/technology/network. The word 'bitcoin' (no capitalisation) is used when referring to the unit of currency.

merchants and investors.

In November 2008, a paper published on the Internet under the name 'Satoshi Nakamoto' (Satoshi) and titled 'Bitcoin: A Peer-to-Peer Electronic Cash System'<sup>2</sup> introduced the use of a peer-to-peer network<sup>3</sup> to generate what was described as 'a system for electronic transactions without relying on trust'. On 3 January 2009, the Bitcoin network came into existence with the release of the first open source Bitcoin client and the issuance of the first bitcoins.<sup>4</sup>

The main feature that differentiates Bitcoin from any other previous attempts at creating a digital currency is its decentralisation. It uses peer-to-peer technology to transfer value among users without the involvement of a central authority, bank or any other financial institution. The software running the network is open-source. Its code is public, open to contributors and developers, and it is not owned or controlled by a single entity but rather by a community of people. The managing and clearing of transactions and the issuing of new bitcoins is done collectively by a network of people that voluntarily shares the computing power of its machines to run the system. These activities are part of a process called 'mining'. Computers running the network verify and record transactions in a public and shared ledger in which every transaction that ever occurred is recorded permanently and irreversibly. For this activity the volunteers are rewarded with newly minted bitcoins and transaction fees.

The backbone of this network is the cited public ledger of transactions, called the 'blockchain'. The blockchain records every bitcoin transaction in a series of smaller units called 'blocks', which are chronologically ordered

and concatenated to each other and serve to timestamp the transactions they contain and confirm their validity. A new block is added roughly every 10 minutes when one of the computers connected to the network wins a race against all the others in solving a mathematical problem.<sup>5</sup> The reward for having found the solution is a number of bitcoins that halves every four years, thus posing a limit to the number of currency units that will be created (21 million bitcoins). Mining is not the only way one can acquire bitcoins in the same way that mining gold is not the only way one can obtain the precious metal. Like any other currency, one can receive it in exchange for selling goods or services. Thousands of shops now accept bitcoins, including international brands like Overstock or Expedia. People can also buy bitcoins from other people selling them, directly or through the use of exchanges.

It may be useful at this point to introduce two different pieces of software involved in the use of a cryptocurrency. The first is the keystone of the currency, the software that lets peers connect to each other, share information and collectively update the shared ledger. In the Bitcoin network it is called 'Bitcoin Core', derived from Satoshi's original code and maintained by a community of developers. The second category of software is the so-called 'Bitcoin client', used on a user's computer or smartphone to manage addresses (see below) and send/receive transactions.

## 1.2 Where are one's bitcoins?

Bitcoins are exchanged among people by using a 'bitcoin address', a string of numbers and letters that looks like this: 1FedeAz5x1HUXrCNLbtMDqcw6o5GNn4xqX. Bitcoin addresses are automatically generated by the Bitcoin client (together with a cryptographic key pair) when it is installed on a device. Unlike the banking system where a user typically owns one bank account or just a few, a cryptocurrency user can have as many different addresses as needed. Often addresses are used only once and then

<sup>2</sup> Available at <https://bitcoin.org/bitcoin.pdf>.

<sup>3</sup> A peer-to-peer network is one in which peers are equally privileged and equipotent. Peers make their resources (or part of them) directly available to other peers without the need for central coordination. In such a system, peers are equally suppliers and consumers of resources, unlike the traditional client-server model.

<sup>4</sup> Available at <https://blockchain.info/block/000000000019d-6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f>.

<sup>5</sup> Available at [http://en.wikipedia.org/wiki/Cryptographic\\_hash\\_function](http://en.wikipedia.org/wiki/Cryptographic_hash_function).

**DIGITAL LEDGERS**

A digital ledger, like the one used in the Bitcoin network, contains the initial wealth of everyone in the network and the complete history of all the transactions that ever happened in the network itself. Every time a new transaction is announced, a verification process starts. In the example on the right, if Edward wants to transfer 10 bitcoins to David, the network will check through the entire ledger, verify that Edward does not have sufficient funds and reject the transaction. However, if he publishes a new request for transferring 5 bitcoins to David, this time the network having found that he, in fact, owns 5 bitcoins will authorise it.

blockchain	
Alice 10 - Bob 10 - Charlie 5 - David 15	
Alice sends 5 to Bob	
David sends 5 to Charlie	
Alice sends 5 to Charlie	
Bob sends 10 to David	
David sends 10 to Bob	
Bob sends 5 to Edward	
David sends 5 to Edward	
Edward sends 5 to Alice...	
Edward sends 10 to David	✓
Edward sends 5 to David	✓

discarded to maintain privacy. Each transaction recorded in the blockchain simply associates a balance with an address and its public-private key pair. The balance reflected by an address in the blockchain belongs to and can be spent by anyone who has the address's private key and can sign a transaction with it - like using a password to access one's bank account. Users can send bitcoins to other users by using the Bitcoin client running on a computer, a cell phone or any similar device. When the sender initiates a transaction this information is notified to the network. In turn, the network certifies the validity of the transaction, verifying that it has been signed properly with the correct private key and that the transferred value has not been spent in the past. Since the balance is nothing more than a series of transactions recorded in the public ledger, there are no physical 'coins', and the client used to perform transactions does not store any value. Bitcoins are simply an entry in the blockchain and the bitcoins' owner is, in fact, the mere owner of a private key that allows him to sign a transaction. As will be seen, this concept poses serious difficulties and concerns when an amount of bitcoins involved in a criminal activity needs to be seized or confiscated.

**BITCOIN ADDRESSES**

Like writing an email, if one wants to send bitcoins to someone else, he needs his *bitcoin address*. This information will help the network to update the ledger and write down who is the new owner of the amount being transferred. And just like email addresses, one can have as many bitcoin addresses as one pleases because they are created automatically by the bitcoin client used. Addresses come in the form of a 26-35 alphanumeric string of characters beginning with 1 or 3.

**1.3 Legislative characteristics**

The popularity of Bitcoin is increasing. There is now a wide community of people and merchants engaging in the exchange of the currency for virtual and physical goods. The world is beyond the stage when this was merely a curious topic and peculiar online experiment. Bitcoin is used frequently as a currency, and it is attracting huge investments.

Many things have changed since the first purchase was

made using bitcoins in 2010.<sup>6</sup> The market has reached a cap of several billion USD, bitcoins are accepted by more than 50,000 merchants around the world and investments exceeding USD 300 million in the first months of 2014 alone are fuelling new start-ups developing the Bitcoin infrastructure and software. As a new and radically different financial instrument, bitcoin's legal status has changed constantly and rapidly over time, being defined alternatively as a currency, a commodity, a digital asset and so on.

Most countries at present do not have an official policy or definition regarding bitcoins, though governments are beginning to take note of it and are discussing the issue. Although a few of them have warned banks and companies against dealing with bitcoins (for example China, India, Bolivia and Lebanon, among others<sup>7</sup>), so far the general attitude adopted by governments and central banks is a *laissez-faire* approach. Under such a framework, bitcoins are not treated as a currency in terms of state law, and citizens can use them to buy and sell goods and services free from regulatory interference. Bitcoin exchanges, however, which typically operate exclusively online, are often required to register as money transmitters and follow proper KYC regulations. This is changing yet again and governments, especially the United States of America (USA), are seriously considering issuing a 'BitLicense' to businesses that use the new currency in order to enhance customer protection and to avoid catastrophic losses (like the recent bankruptcy of the once biggest bitcoin exchange, the Japan-based Mt.Gox).<sup>8</sup> Clearly, regulating Bitcoin also aims to prevent money being exchanged into the virtual currency to avoid taxation. The Internal Revenue Service (IRS) of the USA and several other tax authorities all over the world are issuing contrasting rulings subjecting bitcoins to different tax regimes. Lastly, regulations are needed to fight another obvious phenomenon – the use of bitcoin and other digital currencies for criminal purposes.

## 2. Tracing digital currencies

### 2.1 Bitcoin and criminals

After warnings by the Financial Action Task Force (FATF),<sup>9</sup> a further paper directly addressed the threat posed by digital currencies in their use to facilitate criminal activities. In April 2012, the Federal Bureau of Investigation (FBI) of the USA issued an intelligence assessment entitled 'Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Detering Illicit Activity.'<sup>10</sup> The assessment states:

Since Bitcoin does not have a centralized authority, law enforcement faces difficulties detecting suspicious activity, identifying users, and obtaining transaction records – problems that might attract malicious actors to Bitcoin. Bitcoin might also logically attract money launderers and other criminals who avoid traditional financial systems by using the Internet to conduct global monetary transfers.

In fact, criminal organisations had already used digital currencies to effectively launder the proceeds of their crimes. The greatest example was a Costa Rican payments processor called Liberty Reserve. It willingly accepted highly suspicious deposits, converted them into its own digital currency (Liberty Reserve dollars) and then converted them back again into clean currencies after a process designed to sever the links to their origin. The money laundering activity took place behind a veil of anonymity. Liberty Reserve was eventually shut down in May 2013 but not before it allegedly laundered USD 6 billion. Unlike Liberty Reserve, Bitcoin is a decentralised and peer-to-peer network. There is no company or Chief Executive Officer (CEO) that can be served a court order to reveal the identity of the owner of addresses used to funnel the proceeds of illicit activity. Seemingly, there is no central 'bitcoin account' that can be seized and confiscated nor is there a main server that

6 Available at <http://www.forbes.com/sites/ericmack/2013/12/23/the-bitcoin-pizza-purchase-thats-worth-7-million-today/>.

7 Available at [http://en.wikipedia.org/wiki/Legality\\_of\\_Bitcoins\\_by\\_country](http://en.wikipedia.org/wiki/Legality_of_Bitcoins_by_country).

8 Available at [http://en.wikipedia.org/wiki/Mt.\\_Gox](http://en.wikipedia.org/wiki/Mt._Gox).

9 Available at [http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF\\_Recommendations.pdf](http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf).

10 Available at [http://www.wired.com/images\\_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf](http://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf).

can be shut down.

## 2.2 The blockchain as an investigative tool

It is generally perceived that the Bitcoin network allows anonymous and untraceable transactions, and criminals can use the currency to move their funds undetected. Of course, this has triggered harsh discussions and bitter debates, thanks also to an uninformed and sensationalistic media campaign. Gavin Andresen, chief scientist of the Bitcoin Foundation, stated:

Bitcoin transaction privacy is really complicated. If you want to be sure that your transactions are going to be private, then you probably need to hire a cryptography PhD to analyse your system.

Although transactions are linked to pseudonymous strings of characters rather than names, they are clearly visible in the blockchain and irreversibly and simultaneously stored in thousands of computers and servers where they can be easily accessed and analysed by everyone, including law enforcement agencies (LEAs). If a single transaction or an address is tied to an identity, it becomes a trivial exercise to follow the financial flows through the blockchain. Think about an author writing several books under a pseudonym: if his name is finally revealed, any book he wrote can now be attributed to him. This does not mean that the identification of the ownership of an address is an easy task, but past experience has proven that it is not impossible. Unlike cash, a digital transaction always leaves a trace, and once the veil of secrecy is pierced, assets can be sought, found and confiscated. As recognised by its core developers, achieving reasonable anonymity with Bitcoin can be quite complicated and perfect anonymity may be impossible. While it may provide a degree of privacy not found in any other means of online payment, a sufficiently motivated entity can analyse and reconstruct a suspect's bitcoin transaction activity. In his original paper,<sup>11</sup> Satoshi recommended the use of a brand new address for every transaction performed to

avoid each transaction being linked to a common owner. Although this remains the suggested best practice, it is not enough to guarantee full anonymity due to other peculiar characteristics embedded in the Bitcoin code.

## 2.3 Investigative techniques

Despite what is generally believed and what the media often suggest, Bitcoin is not designed to launder money or to hide income from taxation, and it is not inherently anonymous. For a well-motivated and skilled computer user, it may be possible to conduct transactions in such a way as to obscure his identity, but in most cases users and their transaction history can be identified. Bitcoin transactions are definitely less anonymous than cash transactions.

Many academics have published studies in which they explain and put to the test several strategies and techniques aimed at analysing the blockchain and tying addresses to their owners. The findings resulting from this research, combined with the intrinsic properties of the Bitcoin protocol and old investigative techniques, can provide investigators and prosecutors with useful and powerful tools to ultimately trace assets hidden through the blockchain.

### 2.3.1 Using the properties of transactions to establish links

As described above, the Bitcoin protocol does not transfer value among users by moving actual 'coins'. A person owns bitcoins if there is a transaction in the blockchain sending money to an address that he controls by possessing its associated private key. When looking at that transaction in the blockchain, it will show its input/s (the origin of the bitcoins sent), its value, a timestamp (certifying once and forever when that transaction occurred) and its output/s (the destination of the bitcoins sent). Inputs and outputs can be more than one because of the way bitcoins are sent and received. A few examples can clarify this point. As a

<sup>11</sup> See supra note 4.

reference, transactions that happened in block #216000<sup>12</sup> will be examined. In this block, one can find the easiest example of a transaction with one input and one output.

In the example provided in figure 1, User A sent 0.1 bitcoins (BTC)<sup>13</sup> from his address 1F58q1<sup>14</sup> to the address 17N24E. This means that User A had in one of his addresses exactly the sum he wanted to transfer to the recipient of the transaction (which can be User A himself or a different User B). But what if User A does not have any single address with the sum he intends to transfer? In this case, instead of sending smaller amounts in independent transactions, he can use different addresses he owns and combine them in a single transaction with more than one input, as in the example below taken from the same block.

In figure 2, a multiple-input transaction is shown. From an investigative point of view, this property of the Bitcoin protocol is extremely important. Since the sender of the BTC 7.9595 signed a transaction involving two inputs from two different addresses, one can safely assume that he owned the private keys associated with both and was therefore the owner of the amount reflected in those addresses. If the identity of any of the addresses involved in a multi-input transaction is revealed, all other addresses are also identified. Often bigger transactions require several different inputs to be combined, leaking the ownership of them all. The following example highlights another important feature of the Bitcoin protocol.

In figure 3, User A wanted to send BTC 25 from his address 15jqbo to the address 1KRjBS. Unfortunately, he did not have an address with the exact balance but one with slightly more

bitcoins (25.3823). In this case, a property of the protocol allows the automatic creation of a 'change address' by the sender's client. When the input is higher than the intended amount, a new address (and its associated private key) is created by the client to receive back the 'change'. This new address is obviously owned by the same person who originated the transaction and whenever this amount is spent or consolidated with other addresses in a new transaction, all the resulting transactions will be easily linked to the same owner of 15jqbo. When several inputs and a 'change address' are present in a transaction, even more addresses can be safely attributed to the same entity, as in figure 4.<sup>15</sup>

12 Available at <https://blockchain.info/block/00000000000001f79a2db-15d0ec6d951729e044749372caf504679bba5b1e65e>.

13 'BTC' is a colloquial abbreviation for bitcoins. Following ISO 4217, a standard published by the International Organisation for Standardisation (ISO) that delineates currency codes, in the future bitcoins will probably be traded as 'XBT', where the prefix 'X' denotes a supranational affiliation.

14 For clarity, Bitcoin addresses will be referred to using their first six digits.

15 In a paper published in 2011 (available at <http://arxiv.org/pdf/1107.4524.pdf>), researchers from the University of Dublin applied the above-mentioned techniques to the alleged theft of approximately 25,000 bitcoins reported in the Bitcoin forum by the forum member 'Allinvain' (available at <http://forum.bitcoin.org/index.php?topic=16457.0>). The outlined analysis successfully follows the path taken by the thief(ves) to try to launder the stolen funds and disguise the origin of the money. Although the study fails to reveal the final identity of the thief due to the missing authority and powers to legally obtain crucial information from businesses, the very same investigation in a case involving money funnelled through bank accounts in several jurisdictions would have taken months and would have required extensive effort in preparing and sending out a great number of mutual legal assistance (MLA) requests, possibly to non-cooperative countries. In another paper released in 2013, 'A Fistful of Bitcoins: Characterizing Payments Among Men with No Names' (available at <http://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf>), a group of researchers from the University of California made use of some of the features outlined above to identify the ownership of more than a million Bitcoin addresses, primarily owned by exchanges and online markets.

Developed by Michele Spagnuolo and available at [http://fc14.ifca.ai/papers/fc14\\_submission\\_11.pdf](http://fc14.ifca.ai/papers/fc14_submission_11.pdf).





### 2.3.2 Using the exchanges to collect information

Although these entities may have operated in the past in a manner suited to the Wild West with little or no obligations, all exchanges are nowadays obliged to implement KYC controls and, in many countries, to be registered as money transmitters. Based on these requirements, it is assumed that digital currency exchanges can become useful partners in a law enforcement investigation. With their assistance, investigators and prosecutors may have access to more information about transacting parties than merely their Bitcoin addresses, such as:

- Contact information: name, date of birth, address, telephone, email address, copy of identification document (ID) or passport;
- User information: balance history, log-in (location, time and IP address); and
- Financial information: bank account or credit card numbers used to fund the account or to withdraw funds.

In their 'user agreement' page, Bitcoin exchanges make reference to their KYC policy and advise customers that they could be obliged to reveal customers' information and 'refuse to process or to cancel any pending Bitcoin Transaction as required by law or in response to a subpoena, court order, or other binding government order.'<sup>16</sup>

### 2.4 Case study: Silk Road

Prosecuting digital currency providers and exchanges is in its infancy. Few charges have been filed and no cases have yet proceeded through trial to verdict. One case is particularly interesting as it shows how an illicit activity entirely based on bitcoins can be investigated and prosecuted, although the trial is still pending at the time of writing. It also shows that LEAs do not need a degree in

information technology (IT) to be able to investigate such a case since it involved a great amount of old-fashioned detective work. The material below is taken from the FBI indictment against the alleged perpetrator. As stated before, the trial is still pending, and therefore the suspect must be presumed innocent until proven guilty.

The case refers to the famous online drug market website operating under the name of 'Silk Road'. It was an eBay-like platform that connected drug dealers with customers using the bitcoin currency. Customers received their orders by mail. The fact that bitcoins were the only form of payment accepted reveals how confident the owner of the website (known at the time by the pseudonym of 'Dread Pirate Roberts' or 'DPR'), sellers and buyers were of the anonymity offered by the digital currency. Moreover, the website was accessible only with the use of an application called 'The Onion Router' (TOR), an anonymising network aimed at preventing traffic analysis. Amongst the goods available on the website (there were thousands of products for sale in the spring of 2013) 70 per cent were drugs. But there were also more than a hundred listings for 'services', like tools for hacking into social networks, hundreds of listings for pirated content, hacked Amazon accounts and fake driver's licenses and passports.

It all started a few months after Silk Road went online. In June 2011, Senator Charles Schumer from the USA publicly asked federal agents to investigate it. They did so and began making several undercover purchases from the site in November 2011. They also did an Internet search and found on a forum a post from early 2011 in which a user named 'altoid' mentioned and advertised Silk Road. Some time thereafter, the same username made another post about Silk Road on another online forum, 'Bitcointalk', seeking help in developing a Bitcoin start-up company. The user also posted his alleged real email address, rossulbricht@gmail.com. The FBI subpoenaed Google for the Gmail address, which was registered to a man named Ross Ulbricht (Ulbricht) and included a pho

<sup>16</sup> Available at [https://coinbase.com/legal/user\\_agreement](https://coinbase.com/legal/user_agreement).

to which matched the one on his LinkedIn profile. The records also showed the IP address used to access the account, leading to an apartment in San Francisco where Ulbricht had moved in September 2012. Previously, in March 2012, he allegedly opened an account under his own name on another website, posted some computer code (later found in the Silk Road source code) and sought advice for fixing a problem. The poster realised his mistake and deleted his real name, but it was too late to go unnoticed. In July 2012, investigators located Silk Road's servers in Iceland, Latvia and Romania, and wrote an MLA request that allowed them to receive a copy of the server, together with records of 1.2 million transactions and all the site operator's email exchanges.

In the meanwhile, an FBI agent went undercover posing as a drug dealer who wanted to do business on Silk Road and DPR allegedly instructed one of his employees to assist. The alleged buyer, who was the employee, arranged a shipment to his home and federal agents arrested him after receiving the drugs. As soon as DPR learnt thereof, he contacted the undercover agent and allegedly asked him to have his employee executed for fear of the possible information he could have given to the FBI. Court papers say he paid USD 80,000 for the hit. As a last piece of the puzzle, in July 2013, customs agents intercepted a package with nine fake IDs, all allegedly with the same picture of Ulbricht. A few days later, investigators visited him in San Francisco. Court papers say he refused to answer any questions, except to point out that hypothetically anyone could go to the website Silk Road and purchase any drugs or fake identity documents. Finally on 1 October 2013, federal agents arrested him in a public library in San Francisco. Fearing that the content of the laptop he had with him on that day could have been encrypted and therefore not accessible for investigation, the federal agents waited until he logged into his computer before raiding the library.

In this way, they were able to access the private keys of hundreds of bitcoin addresses stored in the laptop

and seize more than 170,000 bitcoins. At this point investigators had to use their IT skills. As stated above (1.2), the mere seizure of a private key does not guarantee the exclusive control of the bitcoins stored in the related bitcoin address unless the holder is sure that nobody else has a copy of that private key. In this case, the investigators did not know whether any other accomplice had a copy of those keys and therefore moved the seized bitcoins to newly created bitcoin addresses. A few months later, in June 2014, the United States Marshals Service successfully auctioned part of those bitcoins (precisely 29,656.51306529). The rest of the bitcoin stash will be auctioned in the course of 2015.

#### **2.4.1 Outcomes from the Basel Institute on Governance's workshop**

In April 2014, the Basel Institute on Governance organised a workshop titled 'Money laundering with virtual currency, a new challenge', that was attended by LEAs from several jurisdictions, representatives from the banking sector and two of the federal agents who took part in the Silk Road investigations. The workshop mainly tackled two key points resulting from the Silk Road case: how evidence can be sought, and how to deal with encrypted evidence. The key outcomes are summarised below:

##### *Cooperation*

As seen from the case study, it is imperative in investigations where several jurisdictions are involved to develop effective working relationships with other countries to facilitate the timely exchange of intelligence. Such relationships allow the requesting authority to understand the particular legislative requirements of the recipient jurisdiction. In this regard, the Council of Europe's Convention on Cybercrime can help in obtaining freezing orders and the retention of data.

##### *Chain of evidence*

Although the blockchain stores and shows a clear and transparent history of all the Bitcoin transactions ever performed through the network and this history can be

analysed to discover an audit trail, investigators must be able to link the suspect's activity with the suspicious transactions under investigation. Surveillance, Internet traffic analysis, forensic analysis of the suspect's IT devices and information obtained from subpoenaed businesses can link his actions beyond reasonable doubt with the illicit activity perpetrated and seen in the blockchain.

Careful consideration must be given to how this material is forensically retained in an evidential format. It must be handled in a scrupulously careful manner to avoid later allegations of tampering or misconduct that can compromise the case. The purpose is to prove that the integrity of the evidence has been maintained from the moment of seizure until its production in court, documenting how the data was gathered, analysed and preserved. Moreover, using the techniques explained above (multi-input and multi-output), suspicious transactions should be sought and analysed against the blockchain. This activity may reveal additional addresses owned by the suspect and expose other potential financial flows and assets.

### 3. Final considerations

Bearing in mind that at present technology limitations preclude the recovery of a missing private key from a known public key (property on which all current encryption standards are based), retrieving the private key of the addresses where the funds to be seized are located becomes fundamental. Whilst in some jurisdictions legislation exists that requires the suspect to surrender the password to allow the decryption of encrypted files, there are several potential difficulties associated with this requirement. In many cases the sentence for failing to disclose a password is as little as two years. In a case like Silk Road, where the ill-gotten funds amount to hundreds of millions of USD, the sentence seems too low to be a deterrent. Moreover, particularly in civil law jurisdictions, that sentence could be completely absorbed by the sentence for the crime from which the funds originated.

Like any criminal investigation, several different strategies can be adopted that, together with a mistake by the suspect, can result in relevant personal details being leaked that will assist in subsequent steps. Due to the way bitcoin addresses work (public/private key pairs) and the frequent use of encryption by tech-savvy criminals to hide the evidence retained on their computers, particular attention must be given to the opportunity to identify passwords, passphrases and private keys by adopting computer forensics or technical and conventional surveillance.

Once secured, the recovered assets must be preserved appropriately. Where allowed by legislation, consideration should be given to exchanging the seized bitcoins into conventional currencies (see 2.4 Case study: Silk Road) due to volatility and potential depreciation of the seized assets. In the past, Bitcoin has seen fluctuations in its rate of 60 per cent in a few hours. When this is not possible, funds should be immediately moved from the seized address due to security reasons. The associated key might have been given to conspirators who would be able to transfer bitcoins elsewhere. Best practice would be to create a new address in a secure manner to avoid the potential manipulation by malware. A secure and non-Internet connected computer should be used to generate a new address and the related private key appropriately secured and documented.

# Notes

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----

-----



A fundamental priority for law enforcement authorities dealing with financial crime is to recover illegally obtained assets and deny criminals access to the proceeds of their crime. The recovery of illegally obtained assets, however, requires first to successfully trace them. Asset tracing refers to the process whereby an investigator identifies, tracks and locates proceeds of crime. In a traditional asset tracing investigation, there are three objectives: locating the assets, linking them to an unlawful activity so as to obtain freezing and confiscation orders, and proving the commission of the relevant offences.

This guide, written by practitioners working for ICAR, is concerned with a practical approach to tracing illegally obtained assets with a strong emphasis on the intelligence and investigatory aspects of asset recovery. It is addressed to an audience with a law enforcement background, including prosecutors, as well as to other practitioners in the field, such as lawyers, financial advisors, investigative journalists and activists.

The chapters of this guide provide practical guidance on the asset tracing process by addressing the pre-investigative and investigative stages, the mutual legal assistance process and the freezing or seizure of assets through the use of the anti-money laundering framework. They also address the use of offshore vehicles and digital currencies as means to hide the source of illicitly obtained proceeds. It is not the intention of the authors to deal exhaustively with the entire process whereby assets are ultimately forfeited or confiscated. However, practitioners can benefit from an easy-to-understand handbook that guides them through the key and critical steps by stressing the strategic considerations as well as crucial 'check-lists' for a successful recovery of illegally obtained assets.