Government of JERSEY

# MONEY LAUNDERING TYPOLOGIES & TRENDS

## JERSEY

**January 2015**

**Jersey Financial Crime Strategy Group**

**Prepared with assistance of Baker & Partners**

HER MAJESTY'S ATTORNEY GENERAL JERSEY

STATES OF JERSEY POLICE

CUSTOMS AND IMMIGRATION JERSEY

JFSC

# Table of Contents

# Glossary of terms

| Abbreviation | Meaning |
|---|---|
| AML/CFT | anti-money laundering/Countering the financing of terrorism |
| CDD | customer due diligence |
| Drug Trafficking Law | the Drug Trafficking Offences (Jersey) Law 1988 |
| FATF | the Financial Action Task Force |
| MLCO | Money Laundering Compliance Officer |
| PEP | politically exposed person |
| relevant person | as defined in Article 1 of the Money Laundering (Jersey) Order 2008 |
| SAR | suspicious activity report |
| the JCIS | the Jersey Customs and Immigration Service |
| the JFCU | the Joint Financial Crimes Unit |
| the JFSC | the Jersey Financial Services Commission |
| the Strategy Group | the Jersey Financial Crime Strategy Group |
| T&CSP | trust and company services provider |
| UK | the United Kingdom |
| US | United States of America |

# 1 Introduction

Jersey's legislative and regulatory strategy to counter money laundering and the financing of terrorism is overseen by the Chief Minister's Department, and is assisted by the *Strategy Group*, which consists of representatives from a number of relevant agencies including the Law Officers' Department, the *JCIS*, the *JFCU* (incorporating Jersey's financial intelligence unit), and the *JFSC*.

This document aims to raise awareness of money laundering methods and techniques relevant to Jersey. Methods and techniques deployed by money launderers and trends identified through typologies are valuable sources of information for the purposes of conducting risk assessments, designing systems and controls (and policies and procedures), calibrating on-going monitoring, and providing training to employees. Where typologies relate to non-resident customers, they need to be understood in the context of the threats and vulnerabilities specific to Jersey in terms of both its status as an international financial centre and the structure of its finance services industry.

This document draws on raw statistical data and information obtained through the *SAR* regime, *AML/CFT* supervision, and successful money laundering prosecutions, which have provided by members of the *Strategy Group*. Data and information provided has been collated and analysed, typologies and trends identified, and then presented as practical guidance for *relevant persons*.

This paper is intended to assist *relevant persons* with the prevention and detection of money laundering and, in particular, to assist *relevant persons* with the identification of customers who may be engaged in criminal activities, and to further improve the quality of *SARs*.

**The presentation of typologies necessarily highlights the potential misuse of services and products offered by Jersey's financial services industry and abuse of legal persons or legal arrangements established in Jersey or elsewhere. However, it is important to bear in mind that the vast majority of these products and services and legal persons and legal arrangements are used for legitimate purposes and, like elsewhere, current intelligence suggests only a small minority are used to launder the proceeds of criminal activity or finance terrorism.**

## 1.1 Money laundering offence

Under the UN Convention against Organised Crime[1], each State Party is required to adopt such legislative and other measures as may be necessary to establish as criminal money laundering offences, when committed intentionally:

> (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;
>
> (b) subject to the basic concepts of its legal system:
>
> (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.

As can be seen from the above, money laundering in its widest sense occurs whenever there are funds that represent the proceeds of a criminal activity and includes any act or attempted act to conceal or disguise the identity of illegally obtained proceeds so that they appear to have originated from legitimate sources. This traditional view of money laundering is that it occurs in three stages: placement, layering and integration.

**Placement** involves physically placing illegally obtained money into the financial system or the retail economy.

**Layering** is the process by which illegally obtained money is separated from its source through a series of financial transactions that makes it difficult to trace the origin.

[1] Similar money laundering offences are described in the Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime.

The final stage of the process, **integration**, involves the conversion of illicit funds into a seemingly legitimate form which may include the purchase of real estate and other assets.

The typologies presented later in this paper highlight the use of *relevant persons* and Jersey legal persons and legal arrangements at the placement and layering stages.

## 1.2 International financial centre

Jersey's financial services industry is a major component of the Island's economy. The nature of the business carried out by the financial services industry brings with it inherent money laundering and financing of terrorism risks, which derive from the characteristics of sophisticated products and services offered to international customers. The industry is dominated by banking, fund administration and *T&CSPs*.

Most customers are non-resident and additional preventative measures to address the risk that such customers present are in place. Nevertheless, given the number of such non-resident customers, money laundering and financing of terrorism risks remain. Figures published by the *JFSC* show the proportion of bank deposits by Jersey residents in March 2014 is 7.1 per cent of the overall total[2]. There is no similar geographical analysis of fund investors as with banking deposits, but the *JFSC's* estimate is that the majority of investors in Jersey administered and managed funds are non-resident.

The resident/non-resident distinction is a familiar challenge in international financial centres, both onshore and offshore, which attract global investors and is reflected in the typologies included in this report.

## 1.3 Domestic predicate offences

Besides the money laundering and financing of terrorism risks arising from the international nature of the financial service industry, locally committed 'street crimes' resulting in laundering of criminal proceeds in Jersey through domestic products and services also feature in typologies included in this report.

[2] Statistics published on the *JFSC* website (March 2014) https://www.jerseyfsc.org/banking_business/statistics/quarterlyanalysis.asp

## 1.4 Financing of terrorism

*SARs* in respect of which financing of terrorism has been suspected tend to be based on an *relevant person's* commercial database search results, news and Google Alerts using key words associated with its customers, or defensive *SARs*, whereby the *relevant person* files a *SAR* following law enforcement contact requesting information. As a result, *SARs* in respect of financing of terrorism do not establish 'classic' typologies.

# 2 Methodology

As part of a previous review of typologies, the *Strategy Group* focused heavily on convictions before the Royal Court.[3] However, cases brought to court are a small proportion of *SARs* made to the *JFCU* and, to be fully representative of the forms of criminal activity suspected, further information is taken into account in this paper.

## 2.1 Data sources

The following sources of information have been used to prepare this paper:

- sanitised *SARs* and thematic reviews presented by the *JFCU*;
- data provided by the *JFSC*;
- cases of money laundering prosecuted locally since 2008, drawing upon sentencing judgments and relevant legislation; and
- data provided by the *JCIS*.

Although *SARs* are generally founded on suspicion rather than fact, the information they contain is indicative of broader trends within the financial services industry. As such, *JFCU* officers have contributed first-hand insight into money laundering trends and patterns derived from *SARs*.

**Part 1** of this paper sets out and evaluates discernible money laundering methods and techniques – identifying typologies. A synopsis of each case is followed by an analysis of the lessons to be learned from an industry perspective. Necessarily, the report gives examples of abuse of position and misuse of legal persons and legal arrangements. **As highlighted earlier, it is important to bear in mind that the vast majority of products and services, and legal persons and legal arrangements, are used for legitimate purposes and only a small minority are misused.**

**Part 2** of this paper gives an overview of one emerging trend: the use of virtual currencies for criminal purposes.

[3] Anti-Money Laundering/Countering the Financing of Terrorism: Typologies from a Jersey perspective (October 2008)

# 3 Money laundering typologies in Jersey

The typologies and warning indicators outlined below are intended to:

- inform *relevant persons* about the various methods and techniques criminals may employ to launder the proceeds of their illicit activity;
- identify areas that require further attention and help *relevant persons* to identify higher risk activities that necessitate monitoring or enhanced monitoring; and
- more generally, assist with the prevention and detection of money laundering.

It is thought that the general effectiveness of Jersey's *AML/CFT* framework has caused criminals to seek alternative ways (and locations) to launder the proceeds of crime. *AML/CFT* measures can therefore never remain static; trends evolve constantly, at a rapid pace, and *relevant persons* have to be flexible enough to manage this reality if they are to successfully prevent and detect money laundering and financing of terrorism.

## 3.1 Tax evasion

For the twelve month period up to the end of September 2014, of a total of 1,632 *SARs* filed, 673 were identified by the *relevant person* as being principally tax-related. The vast majority of these tax-related *SARs* – somewhere in the region of 80-90 per cent – are 'defensive' in their nature. That is to say they are filed in circumstances where the *relevant person* is not aware of any overt indicator of criminality or the existence of any active criminal investigation concerning the customer. This reflects the fact that employees filing *SARs* are not tax specialists and cannot be expected to understand whether the underlying nature of the issue is in fact criminal in nature. Such *SARs* do not establish 'classic' typologies or "warning indicators"; they offer no real insight into suspicion concepts, for example insufficient tax advice, use of complex products or structures, or questions over the legitimacy of funds.

Tax-related *SARs* are generally triggered by events external to *relevant persons* and also as a result of internal monitoring and review procedures. Examples of warning indicators driven by external events include:

- approaches by customers requesting information to comply with a tax amnesty in their home jurisdiction; and

- adverse media coverage or court action in connection with high profile or specialist tax *avoidance* schemes.

With respect to the latter, the increased appetite of governments and regulators to pursue individual and corporate entities in relation to their tax obligations has led to the development of ever more innovative and sophisticated products designed to mitigate and minimise customers' tax liabilities.

The assets held under these products may be administered locally by *relevant persons*; however, the products themselves are often devised and promoted by onshore institutions or intermediaries. The very nature of these products, designed as they are to help retain wealth and minimise tax liability, automatically places them under the scrutiny of their respective tax authorities. Adverse media publicity is likely to cause *relevant persons* to file *SARs* which are, as described above, 'defensive' in character and where there may be no suspicion of tax evasion.

The development of these products must also be considered in light of the recent statement by the Chief Minister, clarifying that Jersey has no wish, or need, to engage with those who seek to involve the Island in aggressive tax planning schemes to avoid *UK* taxation.

Despite the relatively high level of SARs filed in respect of tax, **it is again important to bear in mind that the vast majority of products and services and legal persons and legal arrangements are used for legitimate purposes and current intelligence suggests only a small minority are used for the purposes of criminal activity.**

Warning indicators driven by events internal to a *relevant person* include:

- The presence of longstanding customers with relatively low levels of transactional activity and/or assets of lower value. Where there is no obvious basis for the customer to require an offshore product or service, it may indicate that the product or service is unsuitable for the customer and may not have been disclosed to the customer's tax authority. The landscape of international financial centres has evolved dramatically since the 1970s. The earliest services included unsophisticated financial products that were widely available to *UK* resident customers. Few regulatory criteria were required. Many larger onshore institutions offered offshore accounts to customers as a matter of course.

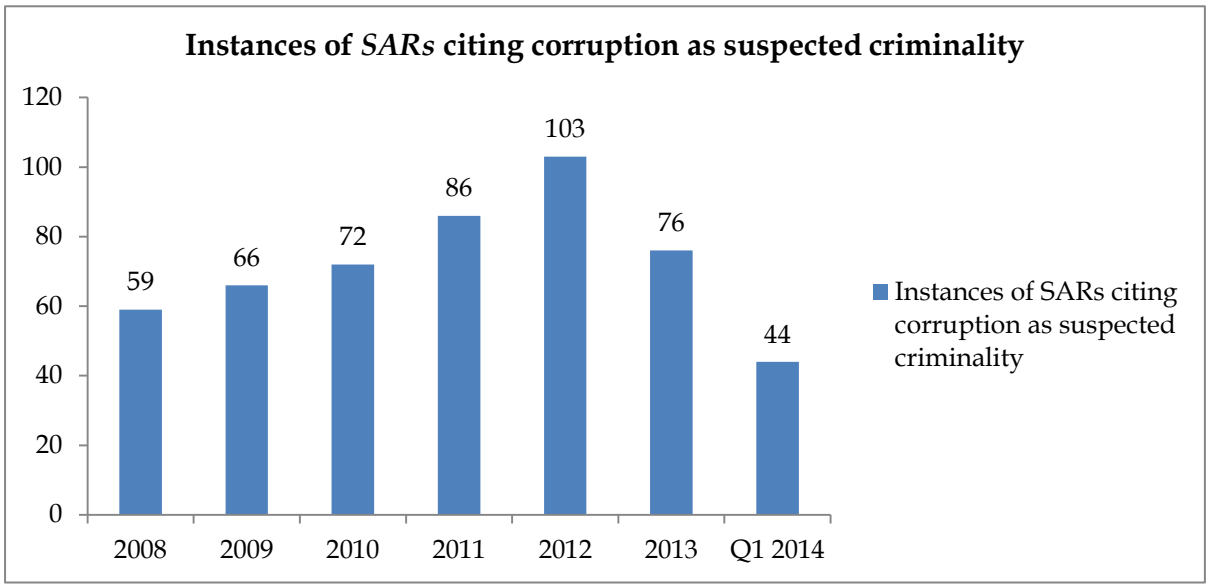
- Where there is reluctance on the part of customers to engage with *relevant persons* or to provide information at a *relevant person's* request, often as a result of internal reviews triggered by requirements to comply with legislation, this may indicate that tax reporting obligations are not being fulfilled or that there is a possibility that criminal tax offences have been committed.

- A failure to respond adequately to questions about tax advice, either concerning legacy accounts, periodic reviews, or due to extraterritorial legislation.

## 3.2 Corruption

In the past six years there has generally been a steady increase in the number of *SARs* citing corruption as the suspected criminality. The first quarter of 2014 suggests that a sharper rise in this trend is currently taking place. Forty-four *SARs* cited corruption as the suspected criminality in this period compared with seventy-six in the whole of 2013. A broader increase in the incidence of corruption being cited since 2008 is demonstrated in the chart below.

**Figure 1: Incidence of corruption as suspected criminality in *SARs* reports**




## 3.3 Laundering the proceeds of corruption with *PEP* involvement

Individuals entrusted with prominent public functions frequently have access to significant public funds and the knowledge and ability to control budgets, public companies and to award contracts. They hold a unique position of influence, which may allow them to circumvent *AML/CFT* measures by influencing, controlling or evading regulations, or awarding contracts in return for illicit personal financial reward.

The global reach of Jersey's financial services industry can pose challenges for *relevant persons* in identifying individuals entrusted with prominent public functions, their close relations and associates (collectively referred to as *PEPs*).

As well as the difficulty of identification, there is sometimes reluctance on the part of *relevant persons* to ask more detailed questions of customers who are *PEPs* about sources of wealth and funds. The absence of such information is revealed in some of the cases when further information is requested by the *JFCU* in support of *SARs* that have been filed, notwithstanding the requirement to apply enhanced *CDD* to *PEPs*. It is important for each *relevant person's* Money Laundering Reporting Officer to understand that requesting further information from a customer as to sources of wealth or funds does not amount to "tipping off" following the filing of a *SAR*.

There is an indication that some members of industry appear to view high net worth individuals with a higher degree of trust and, as such, may ask fewer challenging questions posed where suspicions of wrongdoing exist. This may be due to commercial pressures.

The *JFSC's* on-site examinations have observed this trend; often a *relevant person's* risk rating methodology is found to be too open to subjectivity of the user, which can result in the failure to apply a high enough score to individual risk factors to raise the overall rating of the customer, despite there being a clear need to do so.

**Notwithstanding the identification of this typology, given the global reach of Jersey's financial services industry and client base containing a not insignificant numbers of *PEPs*, the vast majority of products and services, and legal persons and legal arrangements, are used by *PEPs* for legitimate purposes and current intelligence suggests only a small minority are used for the purposes of criminal activity.**

**Corruption typology 1**

Company A is a British Virgin Islands' company specialising in the trading of wines and soft drinks. The company is settled into a Jersey trust administered by a *T&CSP* in Jersey. The managing director of the *T&CSP* is also its *MLCO*.

The settlor of the Jersey trust is the executive chairman of Company A. He is a high net worth individual and prominent businessman domiciled in the Central African Republic. He is reported to have been a significant financial supporter of the current President's election campaign. He has settled a valuable London property into the Jersey trust and also intends to settle a portfolio of shares in the near future. The Jersey trust is in the top 10 per cent of fee earners for the *T&CSP*.

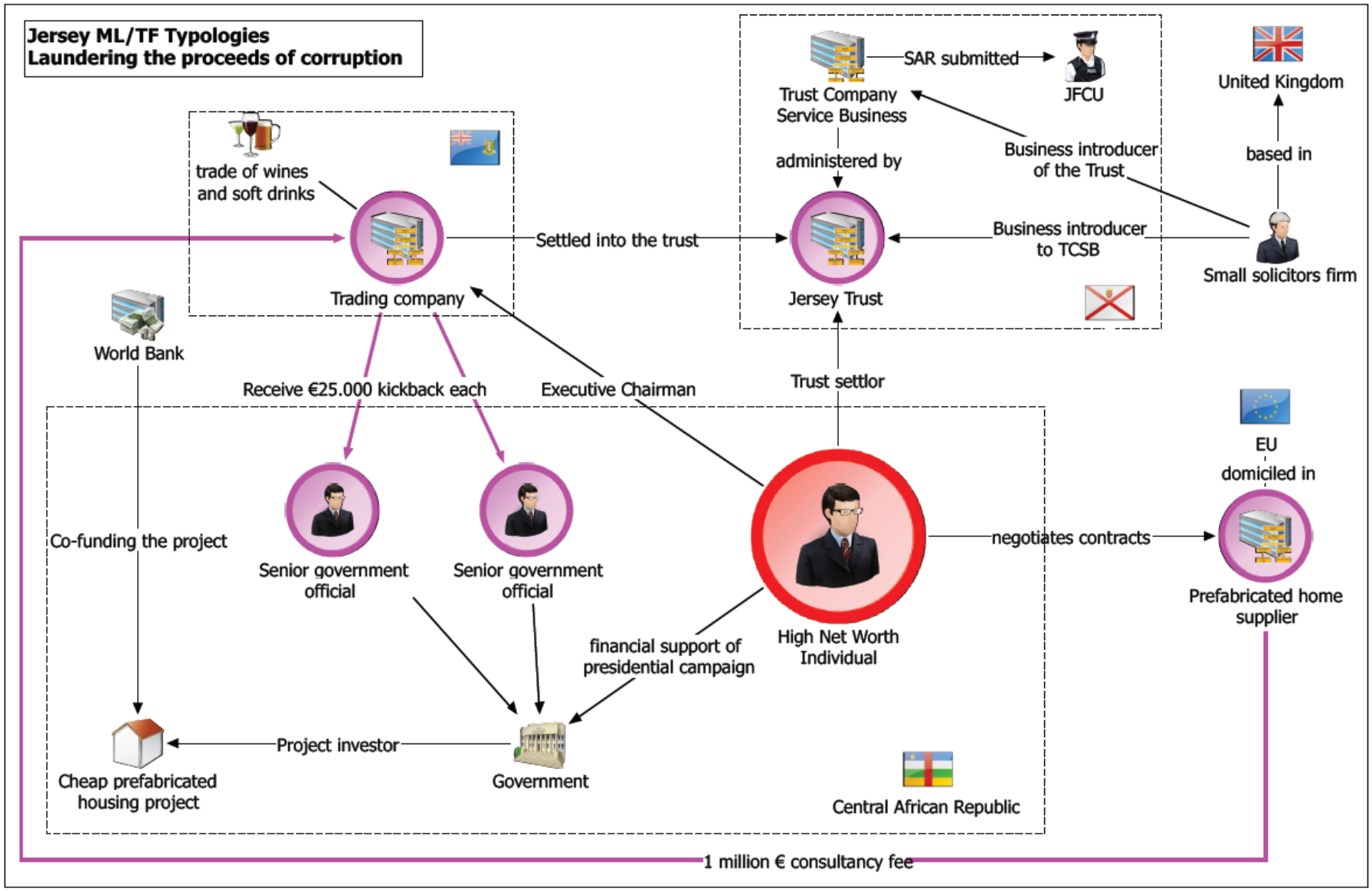
The business relationship was introduced to the *T&CSP* by a small solicitors' firm based in London.

The settlor has been appointed as a special adviser to the African government's housing department and is actively engaged in the negotiation of contracts to secure cheap prefabricated homes for the country's resident population. In participating in such negotiations, the settlor has been engaging with companies located in Europe specialising in providing such homes. The project is being supported and co-funded by the World Bank.

The successful bidder (company based in European Union) pays Company A €1,000,000 as a consultancy fee. Company A then pays €50,000 to key government figures with responsibility for approving the housing project contract in the Central African Republic.

The *T&CSP* files a *SAR* and seeks the advice of the *JFCU*. The *JFCU* issues a "no consent" letter effectively freezing the funds.

A link chart which captures the above information and the linkages between the various parties is produced on the following page.


Jersey ML/TF Typologies
Laundering the proceeds of corruption
Trust Company Service Business
SAR submitted
JFCU
United Kingdom
based in
administered by
Business introducer of the Trust
trade of wines and soft drinks
Settled into the trust
Business introducer to TCSB
Small solicitors firm
Trading company
Jersey Trust
World Bank
Receive €25.000 kickback each
Executive Chairman
Trust settlor
EU
domiciled in
Co-funding the project
Senior government official
Senior government official
High Net Worth Individual
negotiates contracts
Prefabricated home supplier
financial support of presidential campaign
Project investor
Cheap prefabricated housing project
Government
Central African Republic
1 million € consultancy fee

**Warning indicators:**

- The business relationship was introduced by a small firm of solicitors which may have limited compliance resources and could have a vested interest in either assisting the customer (due to other business interests) or putting distance between themselves and the housing project deal.
- By using a British Virgin Islands company settled into a trust, the settlor may be seeking to disguise his connection to the company.
- A small Jersey *T&CSP* was selected to administer the trust where the managing director is also the *MLCO*. Balancing the conflict between the need to secure new customers and the risk posed by a particular customer may be difficult. A small *T&CSP* may be more inclined to accept a high-risk customer in an effort to remain profitable. The customer is an important fee earner increasing the risk that the *relevant person* may be less prepared to challenge the customer on the source of funds.
- A developing African state may be more vulnerable to corruption and the settlor's political connections make him particularly high risk.
- Company A is engaged in buying and selling wines and soft drinks. Receiving €1,000,000 from a company selling prefabricated homes is out of keeping with its business model.
- The settlor could be using the Jersey trust as a vehicle to layer the proceeds of corruption by purchasing a London property and a portfolio of shares.
- As the executive chairman of Company A, the settlor is retaining a high degree of control of business being conducted by the company.
- Receiving a large payment from a firm supplying products to a high risk jurisdiction, followed shortly thereafter by payments to senior government employees engaged in the negotiation of the original contract suggests that Company A's accounts may be used as a money laundering vehicle to launder and distribute the proceeds of corruption.
- The cost of the prefabricated home may have been inflated to cover the €1,000,000 bribe.

**Corruption typology 2**

Mr A is the settlor of a Jersey trust which was established to settle funds that were received from civil engineering contracts in the *US* and Africa.

Mr A fails to mention that he held public office in Mozambique and that he was, in his role as a public official, responsible for awarding construction contracts. As a result of a separate *UK* led investigation, a contractor who admitted making corrupt payments identified Mr A as being responsible for receiving bribery payments.

A review of Mr A's trust accounts identifies that the contractor paid substantial funds into Mr A's Swiss bank account which were then transferred to his bank account in Jersey and then settled into the trust. Mr A was also unable to provide evidence as to the source of his funds and also attempted to hide the existence of the trust from his family.

**Warning indicators:**

- Mr A held public office in a country which was prone to corruption. Notwithstanding the inadequate *CDD* held by the *T&CSP,* which initially failed to positively identify Mr A as being a *PEP*, such information that identified Mr A as being a *PEP* was in the public domain and, the *T&CSP* should have been alerted to the fact that Mr A was connected to a country with corruption problems.
- The commercial rationale for the use of a Jersey trust to receive payments in relation to civil engineering contracts in the *US* and Africa should have been questioned.
- Mr A's position as a public official, which was a matter of public record, gave him the power to award construction contracts. It is not simply the fact that Mr A had *PEP* status, but more importantly he was in a position that was vulnerable to abuse through his ability to award contracts. Further, bribes paid to public officials can often be comparatively small compared to the overall size of the contract and therefore the amount being laundered can appear immaterial despite the level of the corruption. This is particularly true of low level corruption.
- The use of multiple jurisdictions commingled with personal and corporate bank accounts used to channel the funds indicates that Mr A may have been attempting to distance himself from the original source of the tainted funds.

- On questioning, Mr A was unable to provide evidence as to the source of funds. Where customers, who are either prospective or existing, are unable to answer questions and provide evidence as to source of funds, this should immediately raise concerns and increase the risk that money laundering might occur.

**Corruption typology 3**

A government minister, Mr P, from a high risk jurisdiction forms a corrupt business relationship with the chief executive officer, Mr L, of a government utility supplier. Both individuals then begin to accept bribes from foreign business suppliers that are contracted to the utility supplier.

Mr L forms a Jersey registered company (Company R), which is administered by a *T&CSP*. Mr L ensures that he has no public association with this company. Payments from foreign contractors are then paid into the accounts of Company R and then paid into the personal accounts of Mr P and Mr L in Jersey and other corrupt government figures.

Company R recorded these payments under the guise of "commissions" or "consultancy fees". Company R was also unable to provide any proper documentation recording the source of the payments. Payments from Company R's accounts were recorded as either "shareholder dividends" or "interest free loans".

Mr P and Mr L created a further layer by incorporating a company in a different jurisdiction which was then used to receive funds originally transferred from Company R. These funds were then passed on to the final beneficiaries.

**Warning indicators:**

- The use of corporate structures as opposed to holding accounts in personal names without a legitimate rationale can be a warning signal that a money launderer wants to distance himself from the source of the funds. Company R formed a barrier between the accounts of the foreign contractors and those of the personal accounts of Mr P and Mr L. This layering technique was further enhanced when the foreign contractors paid Company R through intermediate companies registered abroad.

- A further use of the technique was evident when Mr P and Mr L created an additional layer by incorporating a company in a different jurisdiction, which was then used to receive funds from Company R. *Relevant persons* should ensure that they understand the rationale behind the use of multiple trusts and companies within a structure. In this case Mr L created complex layers of financial transactions to separate the illicit proceeds from their source and in so doing attempted to disguise the audit trail.
- As Mr L was the chief executive officer of a government utility supplier he was in a unique position to influence the awarding of contracts. The receipt of funds from foreign contractors should elevate the risk of money laundering. A legitimate question to ask would be why an offshore entity is required and why an entity based in the customer's home jurisdiction would not be more appropriate.
- *Relevant persons* should be wary when dealing with structures that involve the receipt of commissions or consultancy fees. These terms are frequently used as euphemisms for bribes or other illicit payments. While not all commissions or consultancy fees constitute illicit payments, *relevant persons* should have a firm and documented understanding of the services that have been provided in order to generate such payments. *T&CSP* that provide director or other fiduciary services need to be equally mindful of their fiduciary duties.
- In a similar vein, the use of interest free loans which have no security or any realistic prospect of repayment should also raise the risk of money laundering. This may be used as a method of facilitating the channelling of funds with little or no prospect of the funds ever being returned to the company.

**Corruption typology 4**

The case of **AG v Bhojwani**[4] highlights various aspects of the corruption typologies identified above, principally the role played by close business associates of individuals holding prominent public functions, the use of bearer financial instruments that allow a degree of anonymity and the inflation of invoiced amounts for goods supplied.

[4] [2010] JRC 116

The Defendant was convicted under the Proceeds of Crime (Jersey) Law 1999 of two counts of converting the proceeds of criminal conduct and of one count of removing the proceeds of criminal conduct from the jurisdiction of Jersey.

In 1996 and 1997, the Defendant negotiated two contracts with the military dictatorship of General Abacha, then the President of Nigeria, for the supply of army vehicles to Nigeria at vastly inflated prices. The illegal surplus of some US$130 million was paid into the Defendant's Jersey bank accounts, from where he transferred large sums to accounts in other countries, including Switzerland, accounts which he knew to be beneficially owned by Abacha family members and others linked to the regime. The Defendant personally made a profit of US$40 million out of the two fraudulent contracts, which he held in the name of his front company at Bank of India (Jersey) between 1997 and 2000.

In October 2000, the Financial Times published a report exposing the late President Abacha's corruption in which they revealed that the Swiss authorities had identified accounts connected with General Abacha into which millions of dollars from Nigerian government corruption had flowed.

The Defendant, aware that those accounts included sums paid through his company, immediately converted all the proceeds of the accounts he controlled at Bank of India, totalling $43.9 million, into freely negotiable drafts. These he then had delivered to London. The sums remained out of the banking system for 12 days before the Defendant delivered the drafts back to Jersey to be credited to accounts in the names of different companies under his control.

After a lengthy trial, the Royal Court found that each of these transactions had been undertaken for the purposes of avoiding prosecution for an offence in Jersey, or the making or enforcement of a Jersey confiscation order against him.

The Bhojwani case demonstrated the potential difficulties in prosecuting complex, multi-jurisdictional offending, and thus the necessity of identifying issues in a timely fashion and gathering evidence early. Quite often, by the very nature of the offending, those being prosecuted have considerable resources and influence both in Jersey and beyond, which they will seek to deploy in trying to avoid the consequences of their crimes. The defendant's legal team used an array of applications and challenges throughout the proceedings, from abuse of process and jurisdictional arguments to judicial review of prosecution decisions.

To help reduce the difficulties in bringing any subsequent prosecution, *relevant persons* should be aware of the absolute requirement to make *SARs* at the earliest possible opportunity.

The ability to prosecute such a case depended greatly on evidence that could be obtained from Nigeria, such evidence being relevant to the underlying criminality and the subsequent laundering of the criminal proceeds. A large degree of cooperation was essential. There is thus great value in an active and robust *SAR* regime: the intelligence that *SARs* provide is vital in identifying matters that need to be investigated.

Notwithstanding the sums involved, the laundering of proceeds in this case was described by the Royal Court as "amateurish". Money laundering can take many different forms and levels of sophistication. Just as small sums are not necessarily indicative of a less professional enterprise, so large sums do not always display a high level of professionalism. The money laundering in this case was undertaken over a short period in an unplanned reaction to external events.

**Warning indicators:**

- The use of freely negotiable drafts provides a disconnect between the customer and the funds. Any instruments that provide such anonymity should be handled with extreme caution.

- Nigeria is a jurisdiction whose public sector is perceived as having a high level of corruption, as determined by expert assessments and opinion surveys of corruption matters[5]. The Defendant's political connections ought to have easily identified him as a high risk individual. Extra vigilance should be shown by *relevant persons* in *CDD* in cases of this kind.

## 3.4 Money service business and use of prepaid cards

A combination of features make bureaux de change and prepaid cards attractive to criminals; they predominantly involve lower value, cash-denominated transactions with prepaid cards in particular facilitating cross-border movement of funds. The *FATF* has identified a number of money exchange indicators relating to transactions, customer profile

[5] See Transparency International's Corruption Index 2013 ranking Nigeria 144 out of 177 countries

and behaviour, and geographical profile in a typologies report[6]. Bureaux de change need also to be aware of the risks presented by: disconnected *CDD* measures; lack of employee awareness of money laundering and financing of terrorism; and training provided to customer facing employees.

The risks inherent in the use of prepaid cards are set out in Section 4 of the *AML/CFT* Handbooks published by the *JFSC*.

Despite the example typologies identified below, **it is again important to bear in mind that the vast majority of bureaux de change and prepaid card activity in Jersey occurs for legitimate purposes and current intelligence suggests only a small minority are used for the purposes of criminal activity.**

**Money service business typology 1**

In the case of AG v McFeat, Smyth and Howard[7], the Defendants were each convicted under the *Drug Trafficking Law* of one count of assisting another to retain the benefit of that person's drug trafficking, by laundering the proceeds thereof in Jersey.

Their offending formed part of a conspiracy headed by Liam and Richard Norris to import commercial quantities of cannabis resin into Jersey from the *UK*. Around £2.7 million of cannabis resin was seized from premises in Staffordshire when several of the conspirators were arrested in March 2012.

All three Defendants entered guilty pleas on the basis that they suspected the money they were transacting on behalf of a third party to be the proceeds of drug trafficking. Between them, the Defendants laundered over £150,000, McFeat over a period of 34 months and Smyth and Howard (who lived together) over a period of 27 months.

The laundering of those proceeds was accomplished in two ways. First, the Defendants would exchange Sterling for euros (always in amounts below the threshold likely to have prompted a *SAR*) at various post offices throughout the Island. The relatively small individual sums occasionally necessitated many visits to different post offices on the same day.

6 FATF 2010 Report on ML through Money remittance and Currency Exchange Providers

7 [2013] JRC 137

The second method concerned the loading of money in Jersey onto prepaid travel cards, which cards had been issued in the Defendants' respective names. These cards enable the movement of cash between countries. With knowledge only of the required multi-digit number, cash could be "loaded" by the Defendants onto a card which was in the hands of a third party in another jurisdiction. That third party could in turn withdraw the money from the card. Money loaded onto the cards in the names of Smyth and Howard was shown to have subsequently been withdrawn in Staffordshire, while that loaded by McFeat was withdrawn in Spain.

**Warning indicators:**

- The absence of any (or any substantial) remuneration for those alleged to have been laundering the proceeds of drug trafficking does not necessarily indicate that those persons have no involvement in the laundering. There may be other reasons for their involvement, e.g. in payment of a debt, pressure from friends/family etc.

- The Defendants deliberately laundered sums in individual amounts small enough to avoid raising questions by counter staff and attracting the attention of authorities, and over a significant period of time. Although money laundering is often associated with large amounts and using sophisticated techniques, such as the use of corporate vehicles, this case demonstrates that vigilance must be maintained even when dealing with relatively small amounts. This reinforces the need for comparatively junior staff at a *relevant person* to demonstrate a healthy professional scepticism.

**Money service business typology 2**

In the case of AG v Ellis[8], the Defendant is the mother of Liam Norris (referred to in money service business typology 1) and, as with McFeat, Smyth and Howard (see above), she was involved with the conspiracy to import commercial amounts of cannabis resin into Jersey. Liam Norris engaged the services of numerous individuals to launder the proceeds of the importations. The Defendant was convicted under the *Drug Trafficking Law* of one count of assisting another to retain the benefit of that person's drug trafficking.

[8] [2013] JRC 226

Over a 17-month period between 2010 and 2011, the Defendant – who during the relevant period resided in the *UK* – travelled to Jersey and changed a total of £25,133 from Sterling into euros at numerous bureaux de change at Jersey post offices and Co-op stores. She used an expired passport in her former married name on 5 separate occasions to exchange money at Jersey post offices. She also used that name on a further 29 occasions to purchase euros.

The value of the drugs being trafficked was substantial, however the Defendant's own involvement concerned sums of a far smaller value, which it may be more difficult to identify as the proceeds of crime.

**Warning indicators:**

- Given the residence of the Defendant in another jurisdiction, the need to convert Sterling into euros (and vice versa) on a regular basis at bureaux de change in Jersey should prompt questions.
- The attempted use of an expired passport should prompt questions (since it is unlikely to comply with the requirement to obtain evidence from a reliable and independent source set out in Article 3 of the Money Laundering (Jersey) Order 2008).

**Money service business typology 3**

In the case of AG v Figueira[9], the Defendant was convicted under the *Drug Trafficking Law* of two counts of assisting another to retain the benefit of drug trafficking. In the same proceedings she was convicted of contempt of court, having absconded whilst on conditional bail after initially having been charged with drug trafficking offences 7 years earlier.

Over a 17-week period, and in eight separate payments, the Defendant had transferred the total sum of £14,900 in cash to Portugal via Girobank. These transfers had been made from different post offices around the Island, but it had not been possible to trace the final destination of the funds. The Defendant had also opened a bank account in Jersey into which cash payments totalling £5,150 had been made for which there did not appear to be any legitimate source.

[9] [2013] JRC 215

She confirmed that the transferred monies were not hers and belonged to another person, a male, who was currently serving a 7-year prison sentence in Madeira. She declined to identify this individual. In return for her assistance, the Defendant had had her rent paid over the said period in the sum of £2,890.

**Warning indicators:**

- Even where the sums are relatively insignificant, if the source of funds is suspicious this may be an indicator of criminality.
- The rewards of the third party launderer are not always obvious. In this case, the Defendant had her rent paid over the material period at a rate of £170 per week.

# 4 Emerging money laundering trends

## 4.1 Virtual Currencies

Virtual currencies (also known as crypto-currencies**)** are distributed, open-source, maths-based peer-to-peer currencies that have no central administrating authority and no central monitoring or oversight. Examples include Bitcoin, Altcoin, Dogecoin and the like.

An *FATF* discussion paper on virtual currencies issued in June 2014[10] defines virtual currencies as *"a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. A decentralized virtual currency is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency."*

Virtual currencies are not of themselves illegal and indeed the *JFSC* has recently issued a permit for a collective investment fund dealing in Bitcoins. Virtual currencies and in particular Bitcoin may become the 'internet of money' and, the architecture that underpins it, the mainstream payment system and validation protocol of the future. However, it is necessary to identify and manage the risks just as that process has been necessary with credit cards and other transactional cards.

The distinct features of virtual currencies and vulnerabilities that criminals currently seek to exploit the most are:

- virtual currencies may allow greater anonymity than traditional non-cash payment methods, as they can be traded on the Internet in non face-to-face relationships and may permit anonymous funding of illicit activities;

- virtual currencies may also permit anonymous transfers due to the lack of formal identification of sender and recipient;

- virtual currencies allow almost instantaneous global reach and greater anonymity than traditional electronic money-based products. For example, Bitcoin protocol does not require or provide identification and verification of participants or generate historical records of transactions that are necessarily associated with real world identity;

[10] See *FATF* Report : Virtual Currencies – Key definitions and potential *AML/CFT* risks – June 2014

- virtual currencies commonly rely on complex infrastructures that involve several entities, often spread across several countries, to transfer funds or execute payments making policing and monitoring transactions extremely difficult;
- use of additional software and anonymisation techniques that obscure the source of a virtual transaction and facilitate anonymity;
- there is no central oversight body, hence there is no centrally deployed monitoring system which can identify suspicious transactions; and
- law enforcement is unable to identify one central location for investigative or asset seizure purposes.

Recent law enforcement actions outside Jersey against virtual currency system participants have included:

- criminal charges brought against Liberty Reserve, a Costa Rica based money remitter, and seven of its principals and employees for operating an unlicensed money service business;
- charges brought against two principals each running a Bitcoin exchange for allowing large quantities of Bitcoins to be purchased and subsequently used to buy drugs on Silk Road, a notorious underground cyber drug-marketplace; and
- a recent seizure of 388 Bitcoins (worth roughly €200,000) from a purportedly illegally operated Bitcoin exchange in France (potential charges on illegal banking, money laundering and operating an illegal gambling website are being considered).

The inherent anonymity of Bitcoin and other crypto-currencies is recognised as a major obstacle for the law enforcement community to trace crypto-currency denominated transactions used to buy and sell various contraband and engage in subsequent laundering activities.

Law enforcement intelligence in Jersey suggests that local individuals ordering controlled drugs from online drug marketplaces have used Bitcoins as a means of payment for the drugs supply. One of the cases featured an online, over-the-counter marketplace platform for trading Bitcoins called Bitcoin-OTC[11] (operating outside Jersey), which was used as a means to obtain Bitcoins.

Bitcoin-OTC is a trusted, online Bitcoin trading platform where registered individuals can either use the order aggregation service provided by the platform or set up trades on a person-to-person basis without interacting with the platform. A wide variety of payment methods ranging from traditional payment methods (wire transfers, credit card payments) to internet based payment systems (PayPal) can be used to purchase or sell Bitcoins via Bitcoin-OTC.

A raft of Bitcoin addresses along with several Bitcoin-OTC traders were engaged by suspects in Jersey to source Bitcoins that were subsequently used as a payment method for drugs on illicit online drug markets. A combination of a completely unregulated online trading platform and a multitude of Bitcoin addresses generated to facilitate the receipt and onward transfer of Bitcoins have emerged as crime facilitating factors just as the Internet has enabled the development of traditional crimes.

In order to address potential opportunities that Bitcoin and other virtual currencies may offer to would-be launderers and terrorist financiers, an in-depth analysis of all relevant *AML/CFT* risks and their key drivers has been prepared for consideration by the *Strategy Group* in order to determine the most effective and proportionate legislative, regulatory and law enforcement response to mitigating risk in this area.

In the meantime, *relevant persons* should apply additional scrutiny to customers whose business activities involve the exchange of, or trade in, virtual currencies.

Members of the *Strategy Group* are also actively monitoring the approach of other jurisdictions and international standard setters to mitigate the *AML/CFT* risks associated with this fast moving area. If an internationally accepted standard is adopted, Jersey will implement appropriate measures to adopt the international standard.

[11] http://bitcoin-otc.com/